INFORMATION SECURITY MODULE HANDBOOK

Module designation	***COMP 101 – Application of ICT in Engineering 1***
Semester(s) in which the module is taught	*Year 1, fall semester*
Person responsible for the module	*PhDc Aygul Musayeva, PhD Rahila Hasanova* *BHOS White city Building ROOM 301* *aygul.musayeva@bhos.edu.az* *rahila.hasanova@bhos.edu.az* *99412 5210000 ext. 33030*
Language	*Native*
Relation to curriculum	*Compulsory* *BSc programms: Computer Engineering, Process automaton Engineering, Information Security, Computer Science*
Teaching methods	*Lecture, Laboratory works, Home Assignments, Quizes, Presentations*
Workload (incl. contact hours, self-study hours)	*Total workload: 300 h = 180 h extracurricular hours + 120 h classroom* ***Classroom hours**:* *Lecture: 60 h (4 h /week)* *Laboratory: 60 h (4 h / week)* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 12 h/ week*
Credit points	*10 ECTS*
Required and recommended prerequisites for joining the module	*No prerequisites, only ordinary school knowledge*
Module objectives/intended learning outcomes	*Each graduated student should be able to:* • *Apply fundamental principles and methods of Computer Science to a wide range of applications* • *Apply mathematical and scientific reasoning to a variety of computational problems* • *Design, correctly implement and document solutions to significant computational problems* • *Work effectively in teams to design and implement solutions to computational problems* • *Communicate effectively, both orally and in writing* • *Think critically and creatively, both independently and with others* • *Recognize the social and ethical responsibilities of a professional working in the discipline* *Adapt to new developments in the field of computer science*
Content	*Information and information processes* - *Informatics and information* - *Measurement of information* - *Information structure*

	Information coding - *Coding* - *Decoding* - *Discretization* - *Information measurement* *Numeral systems* - *Positional numeral systems* - *Non-Positional numeral systems* - *Binary system* - *Octal numeral systems* - *Hexadecimal numeral system* - *Other numeral systems* *Computer logic* - *Logical operations* - *Simplification of logical expressions* - *Synthesis of logical expressions* - *Computer logic gates* *Computer algebra* *-Storing integers in computer memory* *- Storing real numbers in computer memory* *- operation on real and integer numbers* *Hardware* *- computer classification* *- computer generations* *- computer element base* *- memory* *- processor* *- input and output devices* *Software* *- Software classification* *- System software* *- Applications* *Computer networks* - *Network classification and topology* - *Local network* - *Internet network* - *IP address* - *WWW* - *Email*
Examination forms	***Exam*** ***Weight***
	Final *40%*
	Laboratory *20%* *one lab per week*
	Quizzes *20%* *at the end of topic*
	Presentation *20%* *5 & 10 weeks*

Study and examination requirements	***Withdrawal (pass / fail)*** *This course strictly follows grading policy of the Information Technology Department. Thus, a student is normally expected to achieve more than 50% from total score during Final exam and a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred to participate in Resit exam or required to repeat the course the following term or year.* ***Requirements for successfully passing the module*** *1. Attend class regularly, arrive on time, leave only when dismissed* *2. Attend class with all materials required, be prepared to listen and work* *3. Be well prepared for class, read all required materials, and complete all necessary preparation* *4. Be attentive in class, take notes, contribute to discussion and ask intelligent questions* *5. Demonstrate professional and respectful interpersonal relationships with peers and instructor: ATTITUDE COUNTS, AND whining is unacceptable* *6. Take responsibility for your actions, and your results*
Reading list	***Main Textbook****:* 1. *Allakhverdiyeva N.R., Namazov M.B. Computer & Information-Communication Technologies. – 2011, 159 p. (azeri+russian)* 2. *Allakhverdiyeva N.R. Introduction to Databases – 2011, 110 p. (azeri+russian)* ***Recommended Reading:*** 1. *Ron White. How Computers Work.- 2008, 465 p.* 2. *CompTIA A+ Complete Study Guide, 998 pp., 2016* ***Teaching resources*** *Electronic materials placed at Baku Higher Oil School website for this course: Syllabus, PowerPoint slides, exercises, assignments, case studies, announcements, exam samples, and discussions (www.lms.bhos.edu.az).* *Software: Microsoft Office (Word, Excel, Power Point, Access)* *For class presentations and discussions, the student should utilize journal and internet materials. Moreover, the course does not limit the use of learning materials available at BHOS library.*

Module designation	***ENG 101 – English 1***
Semester(s) in which the module is taught	*Year 1, fall semester*
Person responsible for the module	*Head of Department* - Asif Gojayev *BHOS White city Building*

	asif.gojayev@bhos.edu.az> *99412 5210000 ext. 33035*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Seminars, class activity, presentation, achievement tests.*
Workload (incl. contact hours, self-study hours)	*Total workload: 600 h = 300 h extracurricular hours + 300 h classroom* ***Classroom hours**:* *Seminar: 300 h (20 h /week)* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 20 h/ week*
Credit points	*20 ECTS*
Required and recommended prerequisites for joining the module	*No prerequisites, only ordinary school knowledge*
Module objectives/intended learning outcomes	• *Demonstrate effective reading strategies to comprehend academic and technical texts.* • *Apply appropriate academic vocabulary and grammar in written and spoken communication.* • *Produce coherent and well-structured academic writing, including essays and reports.* • *Communicate ideas effectively and confidently in academic discussions and presentations.* • *Employ listening and note-taking skills to understand academic lectures and conversations.* • *Use English language skills to comprehend and discuss topics related to science, technology, and information security.*
Content	• *Course orientation, diagnostic test, introduction to academic English* • *Reading comprehension – main ideas and supporting details* • *Vocabulary development – word forms, prefixes, suffixes, collocations* • *Writing skills – paragraph and essay structure* • *Listening comprehension and note-taking* • *Academic writing – reports, summaries, and essays* • *Speaking skills – pronunciation, fluency, expressing opinions* • *Academic vocabulary – STEM and IELTS-related words* • *Reading for inference and argument understanding* • *Writing portfolio – drafting, revising, and editing* • *Presentation skills – academic and technical topics* • *Integrated skills – reading, writing, listening, and speaking practice* • *IELTS practice – reading, writing, speaking, and listening tasks* • *Review and achievement test preparation*
Examination forms	***Exam*** ***Weight*** ***Date*** *Final* *50%* *TBA (to be announced)* *Achievement test* *20%* *every 3 week* *Presentation* *10%* *TBA (to be announced)*

	Class activity	*10%*	*every week*
	Writing portfolio	*10%*	*TBA (to be announced)*
Study and examination requirements	*Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure, the student can also be given a chance to retake the exam. Resit Exam score (50%) +Before Exam score will remain the same (50%)*		
Reading list	***Main Textbooks*** 1. ***Academic Vocabulary**, Amy E. Olsen – Fifth Edition, 2013* 2. ***Barron's Essential Words for the IELTS**, Dr. Lin Lougheed – Third Edition, 2017* ***Supplementary Materials*** 3. ***IELTS Advantage: Writing Skills**, Richard Brown & Lewis Richards – 2011* 4. ***IELTS Maximiser Speaking**, Alireza Memarzadeh – 2007* 5. ***IELTS Made Easy – Task 1**, IELTS Buddy – 2013* 6. ***IELTS Made Easy – Task 2**, IELTS Buddy – 2013*		

Module designation	***COMP 106 – Application of ICT in Engineering 2***
Semester(s) in which the module is taught	*Year 1, Spring semester*

Person responsible for the module	*PhD. Aygul Musayeva* *BHOS White city Building ROOM 301* *aygul.musayeva@bhos.edu.az* *99412 5210000 ext. 33030*
Language	*Native*
Relation to curriculum	*Compulsory* *BSc programms: Computer Engineering, Process automaton Engineering, Information Security, Computer Science*
Teaching methods	*Lecture, Laboratory works, Home Assignments, Quizes*
Workload (incl. contact hours, self-study hours)	*Total workload: 300 h = 180 h extracurricular hours + 120 h classroom* ***Classroom hours**:* *Lecture: 45 h (3 h /week)* *Laboratory: 75 h (5 h / week)* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 12 h/ week*
Credit points	*10 ECTS*
Required and recommended prerequisites for joining the module	*Basic Computer Literacy, Basic Mathematics, Foundations of Programming Logic*
Module objectives/intended learning outcomes	*Each graduated student should be able to:* • *Explain fundamental programming concepts including data types, variables, operators, control structures, functions, and data structures.* • *Describe Python's syntax, semantics, and runtime environment.* • *Write, debug, and execute Python programs to solve basic computational problems.* • *Apply Python modules and libraries for input/output operations, file handling, and simple data processing.* • *Analyze a given problem, design an algorithmic solution, and implement it using Python.* • *Use modular programming techniques to structure code effectively.* • *Employ Integrated Development Environments (IDEs) such as VS Code, PyCharm, or Jupyter Notebook for Python programming.* • *Utilize built-in Python libraries (e.g., math, random, datetime) and understand the use of external packages via pip.* • *Document and comment Python code according to good programming practices.* • *Collaborate in small groups to develop and test simple Python applications.* • *Demonstrate the ability to learn independently by exploring Python documentation and online resources.*

	• *Show readiness to progress to advanced topics such as object-oriented programming, data analysis, or web development using Python.*
Content	*Round 1: The basics of Python Programming* • *Properties of algorithms* • *Saving a program as a file* • *Writing and running programs with IDE* • *Variables, assignment statements and user input* • *Main data types (int, float, str)* • *Arithmetic operations* • *Standard functions: math, random* *Round 2: Control statements (conditions)* • *The conditional if* • *Logical operators* • *Nested and chained if statement* *Round 3: Loops* • *The for-loop and range functions* • *Nested for loop* • *Formatted output* • *Alternative approach: f-string* *Round 4: More about control statements* • *The repetition statements* • *The while loop* • *Nested while loop* *Round 5: Functions* • *Parameters* • *Return values* *Round 6: Strings* • *String and its methods* • *A string as a function parameter and as a return value* *Round 7: Lists and tuples* • *List and its methods* • *A list as a function parameter and as a return value* • *A tuple as a function parameter and as a return value* *Round 8: Search and sort algorithms* • *Search algorithms: sequential and binary search* • *Sort algorithms: bubble, selection and quick sort* *Round 9: More about lists* • *Multidimensional lists: matrix*
Examination forms	***Exam*** ***Weight*** ***Date*** *Final* *40%* *TBA (to be announced)* *Laboratory* *20%* *every week* *Home assignment* *10%* *every week* *Quizes* *30 %* *at the end of topic*
Study and examination requirements	***Withdrawal (pass / fail)*** *This course strictly follows grading policy of the Information Technology Department. Thus, a student is normally expected to achieve more than 50% from total score during Final exam and a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be*

	referred to participate in Resit exam or required to repeat the course the following term or year. ***Requirements for successfully passing the module*** 1. *Attend class regularly, arrive on time, leave only when dismissed* *2. Attend class with all materials required, be prepared to listen and work* *3. Be well prepared for class, read all required materials, and complete all necessary preparation* *4. Be attentive in class, take notes, contribute to discussion and ask intelligent questions* *5. Demonstrate professional and respectful interpersonal relationships with peers and instructor: ATTITUDE COUNTS, AND whining is unacceptable* *6. Take responsibility for your actions, and your results*
Reading list	***Main Textbook****: Sharifov M., Musayeva A., Hasanova R. Python Programming* ***Recommended Reading:*** *[1] Michael Driscoll. Python 101, ISBN-13:978-0-9960628-1-7, 2016* *[2] Ben Stephenson. The Python Workbook. A Brief introduction with Exercises and Solutions. Springer, 2014* ***Teaching resources*** *pptx presentations : Python Programming (in site: www.lms.bhos.edu.az* *Electronic materials placed at Baku Higher Oil School website for this course: Syllabus, PowerPoint slides, exercises, assignments, case studies, announcements, exam samples, and discussions (www.lms.bhos.edu.az).* ***Software:*** *IDLE Python* *For class presentations and discussions, the student should utilize journal and internet materials. Moreover, the course does not limit the use of learning materials available at BHOS library.*

Module designation	***ENG 102 - English 2***

Semester(s) in which the module is taught	*Year 1, Spring semester (Semester 2)*
Person responsible for the module	*Head of Department* - Asif Gojayev *BHOS White city Building* *asif.gojayev@bhos.edu.az>* *99412 5210000 ext. 33035*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Seminars, class activity, presentation, achievement tests.*
Workload (incl. contact hours, self-study hours)	*Total workload: 600 h = 300 h extracurricular hours + 300 h classroom* ***Classroom hours**:* *Seminar: 300 h (20 h /week)* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 20 h/ week*
Credit points	*20 ECTS*
Required and recommended prerequisites for joining the module	*No prerequisites, only ordinary school knowledge*
Module objectives/intended learning outcomes	• *Understand and analyze academic and semi-academic texts effectively.* • *Apply vocabulary and grammar accurately in writing and speaking.* • *Produce structured paragraphs, essays, and reports.* • *Communicate ideas clearly and confidently in oral presentations and discussions.* • *Listen actively and take accurate notes from academic audio sources.* • *Apply English skills to comprehend and discuss topics related to academic and technical contexts.*
Content	• *Course orientation, diagnostic test, introduction to academic English* • *Reading skills – main ideas and supporting details* • *Vocabulary development – word forms, prefixes, suffixes, collocations* • *Writing – paragraph structure and cohesion* • *Listening comprehension – main ideas and details* • *Writing – essays, reports, and summaries* • *Speaking – pronunciation, stress, intonation, and fluency* • *Academic vocabulary – STEM and IELTS-related words* • *Reading for inference, argument, and critical understanding*

	• *Writing portfolio – drafting, revising, and editing* • *Presentations – individual and group projects* • *Integrated skills – combining reading, writing, speaking, listening* • *IELTS practice – reading, writing, listening, speaking* • *Review and achievement test preparation*
Examination forms	***Exam*** ***Weight*** ***Date*** *Final* *50%* *TBA (to be announced)* *Achievement test* *20%* *every 3 week* *Presentation* *10%* *TBA (to be announced)* *Class activity* *10%* *every week* *Writing portfolio* *10%* *TBA (to be announced)*
Study and examination requirements	*Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure, the student can also be given a chance to retake the exam. Resit Exam score (50%) +Before Exam score will remain the same (50%)*
Reading list	***Required Reading / Textbooks*** 1. *World English 2: Real People. Real Places. Real Language, Kristin L. Johannsen & Rebecca Tarver Chase, 2nd Edition, 2015* 2. *World English 3: Real People. Real Places. Real Language, Christian Lee* 3. *Interactive Vocabulary, Amy E. Olsen, 5th Edition, 2013* 4. *First Steps in Academic Writing, Ann Hogue, 2nd Edition, 2008* ***Recommended Materials*** 1. *IELTS Advantage Writing Skills, Richard Brown & Lewis Richards, 2011* 2. *Collins Listening for IELTS, Fiona Aish & Jo Tomlinson, 2011* 3. *IELTS Maximiser Speaking, Alireza Memarzadeh, 2007* 4. *Master IELTS Visuals, Tahasoni*

Module designation	***MATH 201 - Calculus***

Semester(s) in which the module is taught	*Year 2, fall semester*
Person responsible for the module	*Assoc. Prof. Khanum Jafarova* *BHOS Bibiheybat Campus ROOM 110* *khanum.jafarova@bhos.edu.az*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, seminars, midterm, class tests, tutorials*
Workload (incl. contact hours, self-study hours)	*Total workload: 180 h = 120 h extracurricular hours + 60 h classroom* ***Classroom hours**:* *Lecture: 36 h (3 h /week)* *Seminar: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 10 h/ week*
Credit points	*6 ETCS*
Required and recommended prerequisites for joining the module	• *Basic algebra and equation solving* • *Fundamental trigonometry and geometry* • *Pre-calculus concepts (functions, limits, graphs)* • *Logical and analytical thinking skills* • *Elementary physics (recommended)*
Module objectives/intended learning outcomes	• *Students will know and will be able to differentiate and integrate different functions, to use applications of derivatives in investigating the functions and solving engineering optimization problems. They will also use integrals in calculating the areas and volumes. They will be able to use convergence tests to determine whether the series is convergent or divergent.* • *The students will be able to find partial derivatives of the functions of two or more variables, to determine their stationary points and classify them as maxima, minima and saddle points. They will demonstrate appropriate knowledge in solving optimization problems.* • *They will also learn how to calculate double integrals, interchange the order of integration, rewrite the double integral from Cartesian coordinates to polar coordinates. They will understand the applications of double integrals: volume, average values, mass and center of mass.* • *Students will have strong mathematical reasoning and problem solving skills and apply these skills to the solution of theoretical and applied problems in Engineering.* • *Students will demonstrate a comprehension of technology by understanding how things work on a fundamental level.* • *Students will apply concepts of differentiation, integration, and series to model and solve analytical and computational problems in engineering and information security contexts.* • *Students will be able to demonstrate strong mathematical reasoning and problem-solving skills to analyze, optimize, and*

	interpret functions and systems relevant to information security.
Content	• *Functions. Domain and range of a function. Limit of a function. Continuous functions. Derivative of a function, differentiation rules. Applications of derivatives. Equations of a tangent line and a normal line.* • *Stationary points, increasing and decreasing functions, concave up and concave down functions, maxima and minima, inflection points. Optimization problems. Implicit differentiation.* • *Antiderivative, the indefinite integral. Definition and Basic Properties. Methods of Calculation. Integration by substitution, integration by parts.* • *Integration of a rational, irrational and transcendental functions. Integration by partial fractions. Definite integrals.* • *Applications of definite integrals: area under the curve, area between two curves, volumes. Improper integrals.* • *Sequences and series. Infinite series. Convergent and divergent series. Algebraic properties of infinite series. Tests for convergence. Alternating series test. Power series* • *Approximating functions by polynomials. Maclaurin and Taylor series.* • *Functions of two or more variables. Partial differentiation. Higher order partial derivatives.* • *Using the chain rule to find partial derivatives. Stationary points of the functions of two variables.* • *Classification of stationary points. Maxima, minima and saddle points.* • *Solving optimization problems. Partial differential equations.*
Examination forms	***Exam*** ***Weight*** *Final* *70%* *TBA (to be announced)* *Midterm* *30%* *6th week of the semester*
Study and examination requirements	*Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (70%)+Before Exam score will remain the same (30%)*
Reading list	*[1] Stroud K.A. Engineering mathematics; with additions by Dexter J. Booth, 5th edition, Industrial Press, Inc. New York, 2001(available in BHOS library)* *[2] George B. Thomas Calculus: early transcendentals, 12th edition, 2006* *[3] Croft A., Davison R. Mathematics for Engineers , 3rd edition, 2008* *[4] Mary P Attenborough, Mathematics for Electrical Engineering and Computing, 2003* *[5] Anton Howard, Calculus with analytic geometry, 1992* *[6] Roy Larson, Bruce H. Edwards, Calculus of a Single Variable, 9th Edition* *[7] Roy Larson, Bruce H. Edwards, Multivariable Calculus, 11th Edition*

Module designation	***IS 201 - Information & Cybersecurity Fundamentals***
Semester(s) in which the module is taught	*Year 2, fall semester*
Person responsible for the module	*Lecturer Nihad Alili* *BHOS Bibiheybat Campus ROOM 420* *nihad.elili@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, labs, seminar, class activities*
Workload (incl. contact hours, self-study hours)	*Total workload: 150 h = 102 h extracurricular hours + 48 h classroom* ***Classroom hours**:* *Lecture: 24 h (2 h /week)* *Seminar: 12 h (1 h / week)* *Laboratory: 12 h (1 h / week)* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 8.5 h/ week*
Credit points	*5 ETCS*
Required and recommended prerequisites for joining the module	• *Basic understanding of computer systems and operating environments* • *Fundamental networking concepts (IP, protocols, OSI model)* • *Basic programming or scripting knowledge (e.g., Python, C, or Bash)* • *Familiarity with computer hardware and software components* • *Logical and analytical thinking skills for problem-solving* • *Basic knowledge of data storage and file systems* • *Awareness of internet use, ethics, and digital communication principles*
Module objectives/intended learning outcomes	• *Define and differentiate core concepts and terminology in information security and cybersecurity, including the CIA triad, threats, and vulnerabilities.* • *Explain and analyze cybersecurity principles and mechanisms such as authentication, encryption, and network defenses in real-world scenarios.* • *Identify and classify common cyber threats, malware types, and attack vectors using structured analytical approaches.* • *Perform and document practical activities in log analysis, vulnerability assessment, and digital forensics using industry-relevant tools.* • *Apply security policies, risk management principles, and compliance frameworks to simple case studies.* • *Deliver structured oral and written presentations on cybersecurity topics and collaborate effectively in small groups.* • *Recognize the importance of continuous professional learning and the need to adapt to emerging cybersecurity challenges, standards, and technologies.*

Content	• *Introduction to Cybersecurity* • *Threats, Attacks, and Vulnerabilities* • *Security Principles & Risk Management* • *Identification, Authentication, and Authorization* • *Cryptography Fundamentals* • *Security Policies and Standards* • *Network Security Basics* • *Malware and Social Engineering* • *Application and Cloud Security* • *Security Operations Center (SOC) and Incident Response* • *Digital Forensics and Evidence Handling* • *Emerging Trends in Cybersecurity*
Examination forms	***Exam*** ***Weight*** ***Date*** ***Final*** *50%* *TBA (to be announced)* ***Quizzes*** *20%* *weekly Quizzes* ***Laboratory work*** *15%* *one task per week* ***Presentation*** *15%* *weekly Presentations*
Study and examination requirements	*Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (50%)+Before Exam score will remain the same (50%)*
Reading list	• *Cybersecurity for Dummies (2nd Edition) – Joseph Steinberg* • *Cybersecurity for Beginners (2nd Edition) – Raef Meeuwisse* • *Cybersecurity Essentials – Charles J. Brooks* • *Principles of Information Security – Michael Whitman & Herbert Mattord* • *The Basics of Information Security (3rd Edition) – Jason Andress* • *How Cybersecurity Really Works: A Hands-On Guide for Total Beginners – Sam Grubb* • *CompTIA Security+: Get Certified Get Ahead – Darril Gibson* • *CEH v12 Certified Ethical Hacker Study Guide – Ric Messier* • *Computer Security and the Internet: Tools and Jewels – Paul van Oorschot*

Module designation	***IS 203 - Programming language***
Semester(s) in which the module is taught	*Year 2, fall semester*
Person responsible for the module	*Lecturer Gunel Amrahova* *BHOS Bibiheybat Campus ROOM 420* *gunel.amrahova@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, laboratory works,*
Workload (incl. contact hours, self-study hours)	*Total workload: 150 h = 102 h extracurricular hours + 48 h classroom* ***Classroom hours**:* *Lecture: 24 h (2 h /week)* *Laboratory: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 8.5 h/ week*
Credit points	*5 ETCS*
Required and recommended prerequisites for joining the module	• *Basic computer literacy and familiarity with operating systems* • *Understanding of fundamental mathematical and logical concepts* • *Basic problem-solving and algorithmic thinking skills* • *Familiarity with flowcharts or simple pseudocode (recommended)* • *Interest in analytical reasoning and structured thinking*
Module objectives/intended learning outcomes	• *Explain the fundamental principles of computation and describe the role of programming in solving real-world problems.* • *Apply basic programming constructs such as variables, data types, conditionals, loops, and functions in developing simple Python programs.* • *Use data structures such as lists, tuples, and dictionaries effectively for organizing and manipulating data.* • *Design modular programs using decomposition, abstraction, and reusable functions to improve code structure and maintainability.* • *Implement debugging and testing techniques to identify and correct programming errors efficiently.* • *Apply object-oriented programming concepts, including classes, inheritance, and encapsulation, in designing small software solutions.* • *Analyze and evaluate program efficiency through algorithmic thinking, code optimization, and complexity awareness.* • *Develop functional Python programs that solve computational problems independently and document results clearly.* • *Demonstrate secure coding and debugging practices and show awareness of continuous professional learning to adapt to evolving programming tools and technologies.*

Content	• *What is computation?* • *Branching and Iteration* • *String Manipulation, Guess and Check, Approximations, Bisection* • *Decomposition, Abstractions, Functions* • *Tuples, Lists, Aliasing, Mutability, Cloning* • *Recursion, Dictionaries* • *Testing, Debugging, Exceptions, Assertions* • *Object Oriented Programming* • *Python Classes and Inheritance* • *Understanding Program Efficiency* • *Searching and Sorting*
Examination forms	***Exam*** ***Weight*** ***Date*** *Final exam* *40%* *TBA (to be announced)* *Quizzes* *20%* *weekly Quizzes* *Laboratory work* *30%* *one task per week* *Class activity* *10%* *every lesson*
Study and examination requirements	*Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (40%)+Before Exam score will remain the same (60%)*
Reading list	*The textbook is Guttag, John. Introduction to Computation and Programming Using Python: With Application to Understanding Data Third Edition.*

Module designation	***IS 205 - Operating Systems***
Semester(s) in which the module is taught	*Year 2, fall semester*
Person responsible for the module	*Lecturer Kamran Hasanov* *BHOS Bibiheybat Campus ROOM 420* *kamran.hasanov@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, laboratory work, presentations*
Workload (incl. contact hours, self-study hours)	*Total workload: 150 h = 102 h extracurricular hours + 48 h classroom* ***Classroom hours**:* *Lecture: 24 h (2 h /week)* *Laboratory: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 8.5 h/ week*
Credit points	*5 ETCS*
Required and recommended prerequisites for joining the module	• *Basic knowledge of computer hardware and system components* • *Familiarity with programming fundamentals (preferably in Python or C)* • *Understanding of computer networks and internet concepts* • *Basic command-line usage and file management skills* • *Logical and analytical thinking for troubleshooting and automation tasks*
Module objectives/intended learning outcomes	• *Describe the architecture of the Linux operating system, including kernel, user space, processes, memory, and filesystem components.* • *Explain the working principles of the Unix shell and write shell scripts that use commands, pipes, redirection, variables, and control structures.* • *Create command pipelines and shell scripts to automate routine administrative and data-processing tasks.* • *Build and manage basic Linux services and schedule jobs, documenting the configuration and start/stop procedures.* • *Analyze and control processes and signals (ps, top, kill, nice), and monitor resources to troubleshoot system issues.* • *Configure users, permissions, and packages (apt/dpkg) and maintain system logs for auditing and diagnostics.* • *Use core Linux tools effectively (bash, grep, awk, sed, systemd, cron, journalctl, networking utilities) and document results clearly.*

<table>
<tr><td>Content</td><td colspan="3">What is Linux and Kali Linux?
Terminal and Basic Command Line Usage
File Permissions and Ownership
Package Management (APT & dpkg)
User Management
Process and Resource Monitoring
File Systems and Mounting
Networking Basics and Tools
Log Files and System Logging
What is Nmap and Why is it Used?
Introduction to Burp Suite & HTTP Analysis</td></tr>
<tr><td rowspan="5">Examination forms</td><td>Exam</td><td>Weight</td><td>Date</td></tr>
<tr><td>Final</td><td>40%</td><td>TBA (to be announced)</td></tr>
<tr><td>Quizzes</td><td>20%</td><td>6th week of semester</td></tr>
<tr><td>Presentation</td><td>20%</td><td>presentation per 4 weeks</td></tr>
<tr><td>Laboratory</td><td>20%</td><td>five labs for ten topics</td></tr>
<tr><td>Study and examination requirements</td><td colspan="3">Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (40%)+Before Exam score will remain the same (60%)</td></tr>
<tr><td>Reading list</td><td colspan="3">[1] Sander van Vugt, Red Hat RHCSA™ 8 Cert Guide
[2] William Shotts. The Linux Command</td></tr>
</table>

Module designation	***IS 207 - Networking Fundamentals***
Semester(s) in which the module is taught	*Year 2, fall semester*
Person responsible for the module	*Assoc. Prof. Asim Namazov* *BHOS Bibiheybat Campus ROOM 420* *asim.namazov@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, laboratory work, class activities, presentations*
Workload (incl. contact hours, self-study hours)	*Total workload: 150 h = 102 h extracurricular hours + 48 h classroom* ***Classroom hours**:* *Lecture: 24 h (2 h /week)* *Laboratory: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 8.5 h/ week*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	• *Basic understanding of computer systems and hardware components* • *Familiarity with operating systems (Windows/Linux) and file management* • *Fundamental knowledge of binary numbers and data representation* • *Basic programming or scripting experience (recommended)*
Module objectives/intended learning outcomes	• *Describe TCP/IP networking fundamentals and the roles of core protocols and devices (switches, routers, access points).* • *Subnet IPv4 and IPv6 networks, assign addresses, and verify connectivity using CLI commands.* • *Configure basic switching features (VLANs, trunking, STP) and inter-VLAN routing on lab equipment or simulators.* • *Configure and troubleshoot IPv4/IPv6 static routing and explain dynamic routing concepts at an introductory level.* • *Analyze packet flows and diagnose connectivity issues using tools such as ping, traceroute, ipconfig/ifconfig, and Wireshark.* • *Apply wireless networking basics to design and secure a small WLAN (SSID, authentication, encryption, channel planning).* • *Implement fundamental network security controls (ACL basics, secure device access, password policies) and document configurations.* • *Recognize the importance of continuous learning and adherence to evolving networking standards and best practices.*
Content	• *Introduction to TCP/IP Networking, Fundamentals of Ethernet LANs, Fundamentals of WANs and IP Routing*

	• *Using the Command-line interface, Analyzing Ethernet LAN Switching, Configuring Basic Switch Management, Configuring and Verifying Switch Interfaces* • *Implementing Ethernet Virtual LANs* • *Spanning Tree Protocol Concepts RSTP* • *Inter VLAN routing* • *Perspective on IPv4 Subnetting, Analyzing Classfull IPv4 Networks, Analyzing Subnet Masks, Analyzing Existing Subnets* • *Operating Routers, Configuring IPv4, Addresses and Static Routes,IP Routing in The LAN* • *Understanding OSPF Concepts, Implementing OSPF, OSPF Network Type and Neighbors* • *Fundamentals of IP Version 6, IPv6 Addressing and Subnetting, Implementing IPv6 addressing on Routers* • *IPv6 Routing* • *Fundamentals of Wireless Networks, Analyzing Wireless Architectures* • *Securing Wireless Networks, Building a Wireless LAN*
Examination forms	***Exam*** ***Weight*** ***Date*** *Final* *40%* *TBA (to be announced)* *Project* *30%* *7th week of the semester* *Laboratory* *30%* *one lab per week*
Study and examination requirements	*Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (40%)+Before Exam score will remain the same (60%)*
Reading list	***Required Reading:*** *[1] Data Communications and Computer Networks: A Business User's Approach, Seventh Edition Curt M. White, 2014;* *[2] Todd Lammle - CCNA Routing and Switching Study Guide – 2013;* *[3] James F. Kurose and Keith W. Ross , Computer Networking - A Top-Down Approach Featuring the Internet, 6th Edition , 2012 Addison Wesley;* *[4] Odom W. - Cisco CCNA Routing and Switching 200-120 Official Cert Guide Library – 2013* *[5] Andrew S. Tanenbaum, Computer Networks, 5-th Edition,. Prentice Hall, 201 [2] Alan S. Morris. Measurement and Instrumentation Principles. Third Edition. Butterworth-Heinemann, 2001.* *[6] CCNA 200-301 Official Cert Guide - WENDELL ODOM* ***Recommended Reading:*** *[1] Andrew S. Tanenbaum, Computer Networks, 5-th Edition,. Prentice Hall, 201 [2] Alan S. Morris. Measurement and Instrumentation Principles. Third Edition. Butterworth-Heinemann, 2001.* *[2] Todd Lammle - CCNA Routing and Switching Study Guide – 2013;* *[3] Odom W. - Cisco CCNA Routing and Switching 200-120 Official Cert Guide Library – 2013* *[4] CCNA 200-301 Official Cert Guide - WENDELL ODOM*

Module designation	***AZL 211 - Azerbaijani Language and Art of Speech***
Semester(s) in which the module is taught	*Year 2, fall semester*
Person responsible for the module	*Assoc. Prof. Kamala Mehdiyeva* *BHOS Bibiheybat Campus ROOM 420* *kamala/mehdiyeva@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*Azerbaijani*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, seminars*
Workload (incl. contact hours, self-study hours)	*Total workload: 120 h = 84 h extracurricular hours + 36 h classroom* ***Classroom hours**:* *Lecture: 12 h (1 h /week)* *Seminar: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, self-study = 7 h/ week*
Credit points	*4*
Required and recommended prerequisites for joining the module	*Basic school language course knowledge*
Module objectives/intended learning outcomes	• *Demonstrate fluent and accurate oral and written communication in accordance with the norms of the Azerbaijani literary language.* • *Express thoughts clearly, logically, and coherently in different communicative contexts.* • *Apply the principles of speech culture, etiquette, and ethics in both formal and informal settings.* • *Distinguish between oral and written forms of speech and use each appropriately.* • *Use vocabulary, stylistic devices, and expressive means of the Azerbaijani language purposefully and effectively.* • *Analyze and evaluate examples of speech for correctness, richness, and cultural appropriateness.* • *Develop confidence and rhetorical skills in public speaking and presentations.*
Content	• *Speech culture as an integral part of national culture.* • *Stages of development of speech culture. The art of oratory in ancient and classical times. The art of oratory in Azerbaijan.* • *Azerbaijani language and state care for it.* • *Basic conditions of speech culture. The main requirements for cultural speech.* • *Expressiveness of speech. Intonation. Syllable, stress, speech pause, melodiousness of speech.* • *Principles of training the vocal apparatus. Diction. Elimination of diction defects.* • *Types and forms of speech. Areas of oratory.*

	• *The system of norms of the literary language. Phonetic, lexical, grammatical norms.* • *Orthoepic and orthographic rules.* • *The system of functional styles of the Azerbaijani literary language.* • *Official business documents and their preparation.* • *Speech etiquette and conversational ethics. Means that enrich and strengthen speech.*
Examination forms	***Exam*** ***Weight*** ***Date*** *Final* *40%* *TBA (to be announced)* *Activity* *25%* *Every week* *Presentation* *15%* *9th week of the semester* *Midterm* *20%* *6th week of the semester*
Study and examination requirements	*Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (40%)+Before Exam score will remain the same (60%)*
Reading list	*1. Babayev A. Azerbaijani language and speech culture. Baku, 2011.* *2. Abdullayev N. Fundamentals of speech culture. Baku, 2015.* *3. Demirchizade A. Modern Azerbaijani language. Baku, 2007* *4. Aliyev K. Fundamentals of speech culture and stylistics. Baku, 2001* *5. Zamanov N. Heydar Aliyev's speech culture. Baku, 2013.* *6. Jafarov V. Diplomatic etiquette and speech culture. Baku, 2009.* *7. Nazaroglu C. Win life with your speech. Baku, 2020* *8.R.Abdinova. N.Hüseynova.Azerbaijani language and speech culture.Baku 2020.* *9.N.Mammadli. Business and academic communication in Azerbaijani. Baku 2021.* *10. Jafarov V. Business and academic communication in Azerbaijani. Baku 2022.*

Module designation	***MATH 202 - Probability and Statistics***
Semester(s) in which the module is taught	*Year 2, spring semester*
Person responsible for the module	*Assoc. prof. Khanum Jafarova* *BHOS Bibiheybat Campus ROOM 110* *khanum.jafarova@bhos.edu.az*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, seminars, class tests, presentation, midterm*
Workload (incl. contact hours, self-study hours)	*Total workload: 150 h = 102 h extracurricular hours + 48 h classroom* ***Classroom hours**:* *Lecture: 24 h (2 h /week)* *Seminar: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 8.5 h/ week*
Credit points	*5*
Required and recommended prerequisites for joining the module	• *Basic algebra and mathematical reasoning* • *Fundamental concepts of functions, limits, and derivatives* • *Understanding of basic calculus (differentiation and integration)* • *Analytical and logical problem-solving skills*
Module objectives/intended learning outcomes	• *Students will know and will be able to use statistical methods for data collection, data presentation, data analysis and decision making.* • *The students will be able to solve probability problems applying the rules of probability and three diagrams. They will demonstrate appropriate knowledge in solving the problems on discrete and continuous probability distributions.* • *They will also learn how to calculate a confidence interval for the mean of population, understand some of the basic concepts in hypothesis testing and develop decision procedures for the most frequently encountered testing problems based on a sample from a single population.* • *The students will be able to do regression analysis: to exploit the relationship between two variables so that they can gain information about one of them through knowing the values of the other.* • *Students will have strong mathematical reasoning and problem solving skills and apply these skills to the solution of theoretical and applied problems in Engineering.* • *Students will demonstrate a comprehension of technology by understanding how things work on a fundamental level.*
Content	• *Basic probability and events* • *Conditional probability and Bayes' theorem* • *Descriptive statistics and data presentation* • *Measures of central tendency and spread* • *Random variables and distributions* • *Binomial distribution and probabilities*

	• *Poisson distribution and properties* • *Continuous distributions and normal curve* • *Confidence intervals and estimation* • *Hypothesis testing fundamentals* • *Linear regression and correlation analysis*
Examination forms	***Exam*** ***Weight*** ***Date*** *Final* *70%* *TBA (to be announced)* *Midterm* *30%* *6th week of the semester*
Study and examination requirements	*Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (70%)+Before Exam score will remain the same (40%)*
Reading list	*[1] Ronald E.Walpole, Raymond H. Myers, Sharon L.Myers, Keying Ye, Probability and Statistics for Engineers and Scientists, 9th edition, 2012(available in BHOS library)* *[2] Anthony Hayter, Probability and Statistics for Engineers and Scientists, 4th edition* *[3] Sheldon Ross, Probability and Statistics for Engineers and Scientists, 4th edition, 2009* *[4] T.T.Soong, Fundamentals of Probability and Statistics for Engineers, 2004* *[5] Jay L.Devore, Probability and Statistics for Engineering and the Sciences, 8th edition*

Module designation	***HIST 202 - History of Azerbaijan***
Semester(s) in which the module is taught	*Year 2, spring semester*
Person responsible for the module	*Alamdar Shahverdiyev* *BHOS Bibiheybat Campus ROOM 342* *elemdar.shahverdiyev@bhos.edu.az*
Language	*Azerbaijani*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, seminars, presentation, midterm, class activity*
Workload (incl. contact hours, self-study hours)	*Total workload: 150 h = 90 h extracurricular hours + 60 h classroom* ***Classroom hours**:* *Lecture: 36 h (3 h /week)* *Seminar: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 7.5 h/ week*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	• *Basic school history knowledge*
Module objectives/intended learning outcomes	• *Explain the major historical periods and developments of Azerbaijan and establish accurate cause–effect relationships.* • *Identify and analyze primary and secondary historical sources, assessing their reliability and significance.* • *Compare and critically evaluate different interpretations of historical events through essays or presentations.* • *Demonstrate the ability to communicate historical knowledge clearly in both oral and written forms using appropriate terminology.* • *Apply historical understanding to contemporary issues of national identity, governance, and social ethics with cultural sensitivity.*
Content	• *Theoretical, methodological issues and sources of Azerbaijan history. Prehistoric period in the territory of Azerbaijan. Tribal units and initial state formations in the territory of Azerbaijan. Ancient states in the territory of Azerbaijan.* • *The state of Mannea The state of Atropatena. Ancient Albania.* • *Azerbaijan in the III-IX centuries* • *The formation of Azerbaijan nation. Feudal States of Azerbaijan in IX-first half of XI centuries.* • *The Seljug Empire. The State of Atabegs.Azerbaijan in the period of developed feudalism* • *Mongol yoke in Azerbaijan. Timurid State. Shirvanshahs State in XIII-XIV centuries .* • *The territory ruling by Timurid dynasty The states of Karakoyunlu and Aghgoyunlu.* • *The state of Safavids. Azerbaijan in XVI century.* • *Socio-economic life of Azerbaijan in XVI century.*

	• *Azerbaijan in XVII century.* • *The conversion of Azerbaijan into the international conflict arena. The reign of Nadir Shah Afshar. in XVII century* • *Azerbaijan in the period of Khanates. The second part of XVIII century.* • *Southern Azerbaijan in the XIX and XX century.*
Examination forms	***Exam*** ***Weight*** ***Date*** *Exam* *60%* *TBA (to be announced)* *Homework* *15%* *Every week* *Presentation* *5%* *9th week of the semester* *Midterm* *20%* *6th week of the semester*
Study and examination requirements	*Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (60%)+Before Exam score will remain the same (40%)*
Reading list	*1. Ismail bey Zardabli. The history of Azerbaijan. (from ancient times to the present day), London, 2014.* *2. Swietochowski Tadeusz. Russian Azerbaijan, 1905-1920: The shaping of National Identity in a Muslim Community, 2 edit., Cambridge, Cambridge University Press, 2004; National Consciousness and Political Orientations in Azerbaijan. 1905-1920. From the Conference materials held on in 1980.* *3.Mahmudlu Y. Azerbaijan short history of statehood. Baku, 2006.* *4. Mahmudlu Y., Shukurov K. Garabagh. Real history. Facts and documents. Baku, 2005.* *5. Altstadt, Audrey. The Azerbaijani Turks: Power and Identity under Russian rule: Stanford, 1992.* *6. Tale Heydarov. The Armenian Question in the Caucasus: Russian Archive Documents and Publications (1724-1914). 3 vol. 2011.* *7. Books and articles by R.G.Suny; Sheila Fitzpatrick; Moshe Lewin.*

Module designation	***IS 202 - Computer Architecture***
Semester(s) in which the module is taught	*Year 2, spring semester*
Person responsible for the module	*Lecturer Rashad Amirgunayev* *BHOS Bibiheybat Campus ROOM 420* *rashad.amirgunayev@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, laboratory works, presentation, class activity*
Workload (incl. contact hours, self-study hours)	*Total workload: 120 h = 84 h extracurricular hours + 36h classroom* ***Classroom hours**:* *Lecture: 24 h (2 h /week)* *Seminar: 12 h (1 h / week)* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 7 h/ week*
Credit points	*4 ECTS*
Required and recommended prerequisites for joining the module	• *Basic computer literacy and familiarity with operating systems* • *Understanding of digital logic and binary number systems* • *Fundamental programming experience (preferably in Python, C, or similar)* • *Knowledge of basic computer hardware components (CPU, memory, storage)* • *Analytical and problem-solving skills for algorithm and system design*
Module objectives/intended learning outcomes	• *Explain the fundamental concepts and principles of computer architecture, including CPU, memory, and I/O systems.* • *Analyze data representation and perform conversions between number systems.* • *Demonstrate an understanding of instruction set architecture (ISA) and its impact on system performance.* • *Design basic components of a CPU, such as the arithmetic logic unit (ALU) and control unit.* • *Evaluate the performance of memory hierarchies, including cache and virtual memory systems.* • *Implement simple assembly language programs and understand their execution.* • *Explore and apply concepts of pipelining, parallelism, and multicore processing.* • *Use simulation tools and hardware platforms to implement and test computer architecture concepts.* • *Identify emerging trends and challenges in modern computing technologies.*

	• *Collaborate effectively on practical lab assignments and projects, showcasing problem-solving and technical skills.*
Content	• *Introduction to Computer Architecture* • *Data Representation and Number Systems* • *Instruction Set Architecture (ISA)* • *Central Processing Unit (CPU) Design* • *Memory Hierarchy* • *Input/Output Systems* • *Pipelining in Processors* • *Parallelism and Multicore Processors* • *Advanced Memory Systems* • *Storage Systems* • *Networking and Interconnects* • *Future Trends in Computer Architecture*
Examination forms	***Exam*** ***Weight*** ***Date*** *Final* *50%* *TBA (to be announced)* *Quizzes* *30%* *TBA (to be announced)* *Class activity* *20%*
Study and examination requirements	*Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (50%)+Before Exam score will remain the same (50%)*
Reading list	• *David A. Patterson & John L. Hennessy – Computer Organization and Design: The Hardware/Software Interface* • *John L. Hennessy & David A. Patterson – Computer Architecture: A Quantitative Approach* • *Andrew S. Tanenbaum & Todd Austin – Structured Computer Organization* • *Randal E. Bryant & David R. O'Hallaron – Computer Systems: A Programmer's Perspective* • *Coursera – From Nand to Tetris: Building a Modern Computer from First Principles* • *MIT OpenCourseWare – 6.004 Computation Structures* • *Simulation Tools – RARS, MARS, Ripes, Logisim Evolution* • *IEEE Computer Society & ACM Digital Library Articles*

Module designation	***IS 204 - Introduction to Cryptography***
Semester(s) in which the module is taught	*Year 2, spring semester*
Person responsible for the module	*Lecturer Agha Aghayev* *BHOS Bibiheybat Campus ROOM 420* *agha.aghayev@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, laboratory works, midterm, assignments, presenation*
Workload (incl. contact hours, self-study hours)	*Total workload: 150 h = 102h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24 h (2 h /week)* *Laboratory: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 8.5 h/ week*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	• *Discrete mathematics (sets, functions, modular arithmetic), probability basics* • *Programming in C/Python (comfortable with CLI & dependency management)* • *Network Administration*
Module objectives/intended learning outcomes	• *Understand the foundational principles of cryptography, including encryption, decryption, and cryptographic algorithms.* • *Analyze and evaluate the security of cryptographic systems, identifying vulnerabilities and potential attack vectors.* • *Design and implement cryptographic solutions for data confidentiality, integrity, and authenticity in various applications.* • *Explore cryptographic techniques such as public key infrastructure (PKI), homomorphic encryption, and post-quantum cryptography.* • *Investigate the role of cryptographic protocols in securing communication channels, including SSL/TLS, IPSec, and secure key exchange mechanisms.* • *Gain proficiency in cryptographic toolkits and libraries for practical implementation and experimentation.* • *Evaluate the ethical and legal implications of data protection, privacy, and encryption in real-world scenarios.* • *Develop the ability to make informed decisions regarding cryptographic choices in the context of emerging technologies and evolving threats.* • *Collaborate effectively in team projects to solve cryptography and data protection challenges.*

	• *Demonstrate an understanding of cryptographic concepts through assessments, projects, and practical demonstrations.*
Content	• *Introduction to Cryptography* • *Classical Ciphers* • *Symmetric Cryptography* • *WEP Security* • *Asymmetric Cryptography* • *RSA Algorithm* • *Diffie–Hellman & El-Gamal* • *Public-Key Infrastructure* • *Hash Functions* • *Authentication Mechanisms* • *Authentication Protocols* • *Elliptic Curve Cryptography*
Examination forms	***Exam*** ***Weight*** ***Date*** *Final* *40%* *TBA (to be announced)* *Midterm* *30%* *6th week of the semester* *Assignment* *20%* *every 2 week* *Class activity* *10%* *every week*
Study and examination requirements	*Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (40%)+Before Exam score will remain the same (60%)*
Reading list	*[1] Security engineering : A guide to building dependable distributed systems - Ross J. Anderson, Wiley Publishing, Inc.* *[2] A Classical Introduction to Cryptography - Serge Vaudenay, Springer.*

Module designation	***IS 206 - Object-Oriented Programming***
Semester(s) in which the module is taught	*Year 2, spring semester*
Person responsible for the module	*Lecturer Elchin Salahzada* *BHOS Bibiheybat Campus ROOM 420* *elcin.salahzada@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, laboratory works, project, presentation*
Workload (incl. contact hours, self-study hours)	*Total workload: 150 h = 102h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24 h (2 h /week)* *Laboratory: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 8.5 h/ week*
Credit points	*5*
Required and recommended prerequisites for joining the module	• *Basic algorithmic thinking and data structures* • *Introductory knowledge of IDE use and version control* • *Familiarity with procedural logic (loops, functions, modular decomposition)* • *C programming*
Module objectives/intended learning outcomes	• *Explain the key concepts and principles of object-oriented programming, including encapsulation, inheritance, polymorphism, and abstraction.* • *Design and implement object-oriented solutions using C# and UML to model real-world problems.* • *Apply design principles and patterns to create efficient, reusable, and maintainable software.* • *Develop and test applications using modern development environments and debugging tools.* • *Use advanced programming structures such as classes, interfaces, and data structures effectively.* • *Collaborate and evaluate software projects based on quality, reusability, and adherence to OOP standards.*
Content	• *Basic OOP Concepts (UML, Objects, Classes, Attributes, Behaviors)* • *Encapsulation and Interfaces* • *Relationships and Inheritance* • *C# Development Environment* • *Class Creation and Object Initialization* • *Modules, Packages, and Access Control* • *Inheritance, Polymorphism, and Abstract Classes* • *Object-Oriented Design Principles (DRY, KISS, SOLID, YAGNI)* • *Practical OOP Techniques (Decorators, Magic Methods, Object Manager)*

	• *Introduction to GOF Design Patterns* • *Creational Patterns (Prototype, Factory, Builder, etc.)* • *Structural and Behavioral Patterns (Adapter, Facade, Observer, etc.)* • *Version control and code review discipline* • *Automated unit testing (e.g., NUnit/xUnit)*
Examination forms	***Exam*** ***Weight*** ***Date*** *Final* *40%* *TBA (to be announced)* *Project presentation* *35%* *TBA (to be announced)* *Laboratory* *25%* *one lab per week*
Study and examination requirements	*Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (40%)+Before Exam score will remain the same (60%)*
Reading list	*[1] Object-Oriented Programming using C#: Simon Kendal* *[2] Object-Oriented Analysis and Design with Applications: Booch, Jacobs, Rumbauch* *[3] Design Patterns: Elements of Reusable Object-Oriented Software: Erich Gamma, Richard Helm, Ralph Johnson* *[4] Design Patterns in C#: A Hands-on Guide with Real-World Examples* *[5] www.c-sharpcorner.com*

Module designation	***IS 290 – Industrial Internship 1***
Semester(s) in which the module is taught	*Year 2, spring semester*
Person responsible for the module	*Supervisors of Information Technology Department* *BHOS Campus, office , 418* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Mandatory* *BSc program in Information security*
Teaching methods	• *Industrial practice at an approved organization.* • *Supervision and feedback from company mentor and university supervisor.* • *Independent study, daily reporting, and presentation preparation.*
Workload (incl. contact hours, self-study hours)	*Total workload: 180 h = 180 h extracurricular hours* *Duration 4 weeks (After 4th semester)* - ***Contact hours:***
Credit points	*6 ECTS*
Required and recommended prerequisites for joining the module	• *Information & Cybersecurity Fundamentals* • *Operating Systems* • *Networking Fundamentals* • *Computer Architecture* • *Introduction to Cryptography* • *Object-Oriented Programming*
Module objectives/intended learning outcomes	• *Apply fundamental principles of information and cybersecurity in real-world environments.* • *Configure and monitor operating systems and network infrastructures securely.* • *Analyze and identify vulnerabilities in systems, networks, and applications.* • *Implement security tools such as SIEM, firewalls, IDS/IPS, and endpoint protection systems.* • *Apply basic cryptographic methods for data confidentiality and integrity.* • *Develop small-scale security-related software or scripts using object-oriented programming principles.* • *Prepare professional technical reports and presentations reflecting workplace experience.* • *Demonstrate awareness of ethical responsibilities, safety regulations, and professional conduct in a corporate environment.*
Content	• *Network and system security operations.* • *Vulnerability assessment and incident response basics.*

<table>
<tr><td></td><td>

- *Administration of Linux/Windows systems with secure configurations.*
- *Application of cryptographic tools for data protection.*
- *Use of SIEM platforms (e.g., Splunk, ELK) and firewall management.*
- *Software development and automation for security monitoring.*
- *Workplace safety, health, and environmental protection standards.*
- *Preparation of final report and presentation on internship outcomes.*

</td></tr>
<tr><td>Examination forms</td><td>

Component	***Description***	***Weight***
Performance Evaluation by Company Supervisor	*Evaluation of student's professional behavior, punctuality, and contribution during the internship.*	*33.3%*
Internship Report	*Written report including description of tasks, technologies used, safety compliance, and lessons learned.*	*33.3%*
Presentation and Defense	*Oral presentation before BHOS internship commission (after Turnitin check).*	*33.4%*

</td></tr>
<tr><td>Study and examination requirements</td><td>

Notes:

Total: *100%*

Grading Scale:

A (91–100), B (81–90), C (71–80), D (61–70), F (≤60)

- *Each student is assigned an academic supervisor from BHOS and an industrial mentor from the hosting company.*
- *Students must maintain daily logs of activities.*
- *A final report (approved and signed by the company supervisor) must be submitted to the BHOS academic supervisor within one week after completion.*
- *Students must present and defend their internship experience before the BHOS Internship Commission.*

</td></tr>
<tr><td>Required Documentation</td><td>

Before starting the internship:

- *Internship Notice and Program*
- *Individual Task Sheet*
- *Thematic Task assigned by BHOS Department*

After completion:

- *Daily Logbook*
- *Final Internship Report (signed by enterprise mentor)*
- *Reference Letter from the hosting company*
- *PowerPoint Presentation for Defense*

</td></tr>
</table>

Module designation	***MATH 301 - Fundamentals of Discrete Mathematics***
Semester(s) in which the module is taught	*Year 3, Fall semester*
Person responsible for the module	*Lecturer Fuad Suleymanli* *BHOS Bibiheybat Campus ROOM 420* *fuad.suleymanli@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, seminars, class works, presentation*
Workload (incl. contact hours, self-study hours)	*Total workload: 180 h = 132h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24 h (2 h /week)* *Laboratory: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 11 h/ week*
Credit points	*6*
Required and recommended prerequisites for joining the module	• *Basic algebra and mathematical reasoning* • *Familiarity with functions, sets, and relations* • *Elementary combinatorics and counting principles (recommended)* • *Understanding of basic proofs and mathematical induction concepts*
Module objectives/intended learning outcomes	• *Demonstrate knowledge and understanding of core discrete mathematics topics including sets, functions, relations, logic, graphs, and combinatorics;* • *Apply logical reasoning and proof techniques to analyze and solve mathematical problems;* • *Model and solve computational and real-world problems using discrete structures;* • *Show ability to represent problems algorithmically and reason about their correctness;* • *Develop abstract thinking and rigorous reasoning skills that support further courses in mathematics, computer science, and related disciplines.*
Content	• *Introduction to the Course* • *Sets and Functions* • *Set Operations and Algebra of Sets* • *Algebra of Propositions and Predicate Logic* • *Algebra of Circuits and Boolean Algebra* • *Logic Simplification (SoP, MSoP, Karnaugh Maps)* • *Mathematical Induction (Regular and Strong)* • *Well-Ordering and Structural Induction* • *Finite Sets and Counting Principles* • *Combinatorics (Permutations & Combinations)* • *Relations and Their Properties*

<table>
<tr><td></td><td>

- *Graphs and Trees*

</td></tr>
<tr><td>Examination forms</td><td>

Exam	***Weight***	***Date***
Final	*60%*	*TBA (to be announced)*
Quizzes	*30%*	*6th week of the semester*
Class activity	*10%*	*every week*

</td></tr>
<tr><td>Study and examination requirements</td><td>Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (60%)+Before Exam score will remain the same (40%)</td></tr>
<tr><td>Reading list</td><td>[1] Kenneth H. Rosen, Discrete Mathematics and Its Applications, 8th Edition, McGraw-Hill, 2019.

[2] Susanna S. Epp, Discrete Mathematics with Applications, 5th Edition, Cengage, 2019.

[3] Richard Johnsonbaugh, Discrete Mathematics, 8th Edition, Pearson, 2017.</td></tr>
</table>

Module designation	***MATH 303 - Differential Equations***
Semester(s) in which the module is taught	*Year 3, fall semester*
Person responsible for the module	*Lecturer Hidayat Nusratzada* *BHOS Bibiheybat Campus ROOM 420* *hidayat.nusratzade@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, seminars, class activity ,midterm*
Workload (incl. contact hours, self-study hours)	*Total workload: 180 h = 132h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24 h (2 h /week)* *Seminar: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 11 h/ week*
Credit points	*6 ECTS*
Required and recommended prerequisites for joining the module	• *Calculus: derivatives, integrals, and applications of differentiation and integration* • *Basic knowledge of sequences, series, and functions of one or more variables* • *Algebraic manipulation and solving equations* • *Analytical and problem-solving skills for mathematical modeling*
Module objectives/intended learning outcomes	• *Solve first- and second-order differential equations and apply them to model engineering and cybersecurity-related systems.* • *Utilize Laplace transforms and Fourier series for analyzing dynamic behavior in complex technological and information systems.* • *Demonstrate strong mathematical reasoning and analytical problem-solving skills in the context of engineering and information security.* • *Model and interpret real-world processes using differential equations to predict and analyze system performance.* • *Use computational tools (e.g., MATLAB, Python, or Wolfram) to simulate and visualize solutions of differential equations.* • *Evaluate the stability and behavior of technological or cryptographic systems using mathematical modeling techniques.*
Content	• *Introduction to Differential Equations* • *Separable and Linear First-Order Equations* • *Integrating Factors and Initial Value Problems* • *Modeling with First-Order Equations* • *Exact, Homogeneous, and Bernoulli Equations* • *Second-Order Linear Differential Equations*

	• *Homogeneous Equations with Constant Coefficients* • *Complex and Repeated Roots; Reduction of Order* • *Nonhomogeneous Equations (Undetermined Coefficients & Variation of Parameters)* • *Laplace Transform and Its Applications* • *Systems of Differential Equations and LRC Circuits* • *Fourier Series and PDE Applications (Heat & Wave Equations)*
Examination forms	***Exam*** ***Weight*** ***Date*** *Final* *60%* *TBA (to be announced)* *Midterm* *30%* *6th week of the semester* *Class activity* *10%* *every week*
Study and examination requirements	*Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (60%)+Before Exam score will remain the same (40%)*
Reading list	1. *Boyce & DiPrima – Elementary Differential Equations and Boundary Value Problems (10th Ed.)* 2. *E.D. Rainville & P.E. Bedient – Elementary Differential Equations* 3. *Blanchard, Devaney & Hall – Differential Equations: Dynamical Systems and an Introduction to Chaos* 4. *MIT OpenCourseWare – Mathematical Methods for Engineers (online materials)* 5. *Wolfram MathWorld – Differential Equations and Modeling Resources*

Module designation	***IS 301 - Systems Analysis and Design***
Semester(s) in which the module is taught	*Year 3, fall semester*
Person responsible for the module	*Senior lecturer Khayyam Masiyev* *BHOS Bibiheybat Campus ROOM 420* *khayyam.masiyev@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, laboratory work, class activity, presentation*
Workload (incl. contact hours, self-study hours)	*Total workload: 180 h = 132h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24 h (2 h /week)* *Laboratory: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 11 h/ week*
Credit points	*6*
Required and recommended prerequisites for joining the module	• *Basic programming and software development concepts* • *Understanding of computer systems and databases* • *Fundamentals of networking and information systems* • *Analytical and problem-solving skills for modeling and system design*
Module objectives/intended learning outcomes	• *Elicit and specify functional & non-functional requirements (including security, privacy, and compliance constraints) using user stories/use cases with acceptance criteria.* • *Model systems with UML/BPMN (context, DFDs, class, sequence, state, activity) and validate models with stakeholders.* • *Evaluate feasibility and solution options using cost/benefit, risk and impact analysis; justify selected architecture and technology stack.* • *Design data and UI layers (schemas, ERD, wireframes) and define integration/API contracts.* • *Apply agile practices (backlog, DoD, sprint planning) and manage scope, change, and traceability from requirement to test.* • *Plan and execute verification & validation (test strategy, test cases, defect management); report quality metrics.* • *Communicate findings through professional documentation and presentations; collaborate effectively in multidisciplinary teams.* • *Reflect on ethical, legal, societal, and sustainability implications; recommend risk-aware governance controls.*
Content	• *Introduction to Systems Analysis and Design (SAD)* • *Systems Development Environment and Business Case Analysis* • *Evaluation of System Requests and Feasibility Studies*

<table>
<tr><td></td><td>

- *Managing Systems Projects and Project Management Overview*
- *Agile vs Traditional System Development Approaches*
- *Requirements Modeling and Data/Process Modeling*
- *Object Modeling and Development Strategies*
- *User Interface and Data Design*
- *System Development and Implementation*
- *Cloud Computing Components and Service Models*
- *Blockchain Fundamentals*
- *System Testing and Quality Assurance (Test & Defect Management)*

</td></tr>
<tr><td>Examination forms</td><td>

Exam	***Weight***	***Date***
Final	*40%*	*TBA (to be announced)*
Project	*40%*	*TBA (to be announced)*
Class activity	*20%*	

</td></tr>
<tr><td>Study and examination requirements</td><td>Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (70%)+Before Exam score will remain the same (60%)</td></tr>
<tr><td>Reading list</td><td>

1. *Systems Analysis and Design, 12th edition, Scott Tilley, (2020)*
2. *Agile Model-Based Systems Engineering Cookbook, Dr. Bruce Powel Douglass (2021)*
3. *Modern Systems Analysis and Design, 9th edition, Joseph S. Valacich, Joey F. George (2021)*
4. *Olga Filipova, Rui Vilão, "Software Development From A to Z", Apress (2019)*
5. *"Software Engineering, 10th Edition-Pearson, Ian Sommerville, (2020)*
6. *"Modern Systems Analysis and Design", Joseph S Valacich_ Joey F. George (2025)*

</td></tr>
</table>

Module designation	***IS 303 - Introduction to telecommunications***
Semester(s) in which the module is taught	*Year 3, fall semester*
Person responsible for the module	*Senior lecturer Mehran Hematyar* *BHOS Bibiheybat Campus ROOM 420* *mehran.hematyar@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, laboratory work, class activity, presentation*
Workload (incl. contact hours, self-study hours)	*Total workload: 180 h = 132h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24 h (2 h /week)* *Laboratory: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 11 h/ week*
Credit points	*6*
Required and recommended prerequisites for joining the module	• *Fundamentals of computer networks (TCP/IP, OSI model)* • *Basic programming and simulation tools (e.g., Packet Tracer, MATLAB)* • *Principles of electronics and signal processing (recommended)* • *Mathematical foundations: algebra, functions, and basic calculus* • *Understanding of basic data communication concepts*
Module objectives/intended learning outcomes	• *Explain the fundamental concepts, components, and evolution of telecommunication systems — from wired to wireless, and from early telegraphy to 5G technologies.* • *Identify and compare different transmission media (copper, optical fiber, wireless) in terms of bandwidth, cost, reliability, and real-world applications.* • *Describe and apply multiplexing, modulation, and signaling techniques used in modern telecommunication networks.* • *Analyze the structure and function of communication models such as the OSI and TCP/IP layers and map real-world protocols to these layers.* • *Design and simulate small-scale telecommunication systems (e.g., VoIP, LAN/Wi-Fi, or cellular networks) using simulation tools such as Packet Tracer, MATLAB, or GNS3.* • *Evaluate emerging technologies, regulatory issues, and challenges in telecommunication — including spectrum management, broadband expansion, and IoT connectivity.* • *Students will communicate their designs, analyses, and simulation results effectively through technical documentation, presentations, and collaborative project work*
Content	• *Telecommunication History & Evolution* • *Transmission Media Comparison*

<table>
<tr><td></td><td>

- *Multiplexing Techniques*
- *PSTN vs. VoIP Case Study*
- *OSI Model in Practice*
- *Mobile Evolution Timeline*
- *7. Spectrum Regulation Debate*

</td></tr>
<tr><td>Examination forms</td><td>

Exam	***Weight***	***Date***
Final	*20%*	*TBA (to be announced)*
Quizzes	*15%*	*TBA (to be announced)*
Class test	*15%*	*every week*
Project	*10%*	*TBA (to be announced)*
Midterm	*20%*	*6th week of the semester*
Laboratory work	*20%*	*every week*

</td></tr>
<tr><td>Study and examination requirements</td><td>Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (20%)+Before Exam score will remain the same (80%)</td></tr>
<tr><td>Reading list</td><td>

- *Behrouz A. Forouzan – Data Communications and Networking*
- *Simon Haykin & Michael Moher – Introduction to Analog and Digital Communications*
- *John G. Proakis & Masoud Salehi – Communication Systems Engineering*
- *Roger L. Freeman – Telecommunication System Engineering*
- *Theodore S. Rappaport – Wireless Communications: Principles and Practice*
- *William Stallings – Data and Computer Communications*

</td></tr>
</table>

Module designation	***IS 305 - Database Fundamentals***
Semester(s) in which the module is taught	*3 year, fall semester*
Person responsible for the module	*Assoc. Prof. Mahammad Sharifov* *BHOS Bibiheybat Campus ROOM 412* *mahammad.sharifov@bhos.edu.az* *99412 5210000 ext. 33237*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, seminars, midterms, class tests and activity*
Workload (incl. contact hours, self-study hours)	*Total workload: 180 h = 132h extracurricular hours + 48h classroom* *Classroom hours:* *Lecture: 24 h (2 h /week)* *Laboratory: 24 h (2 h / week)* *Contact hours:* *Examination preparation, consultation, selfstudy = 11 h/ week*
Credit points	*6*
Required and recommended prerequisites for joining the module	• *Basic programming concepts (variables, data types, conditionals, loops, functions)* • *Understanding of fundamental data structures (arrays, lists, dictionaries)* • *Familiarity with computer systems and file management* • *Basic mathematical reasoning and logic*
Module objectives/intended learning outcomes	• *Elicit, model, and normalize data requirements; design relational schemas with keys, constraints, and integrity rules.* • *Write and optimize SQL (DDL/DML/DCL): joins, subqueries, window functions, transactions and isolation levels; interpret EXPLAIN plans.* • *Apply the theory of data models by comparing relational, document, key-value, columnar, and graph models; select an appropriate store for a use case.* • *Implement database-backed applications using a mainstream RDBMS (e.g., PostgreSQL/MySQL) and one NoSQL system (e.g., MongoDB), including indexes, views, and stored routines where justified.* • *Define and enforce security controls: RBAC, least privilege, encryption in transit/at rest, input validation, auditing, and backup/restore policies; explain compliance impacts (e.g., GDPR data subject rights, retention).* • *Diagnose and resolve common operational issues (locking, deadlocks, slow queries) using logs and performance tooling; document findings.* • *Collaborate to deliver a small data system: ERD, schema DDL, seed data, sample queries/report, and a short technical report/presentation.*
Content	• *Introductory concepts of DBMS* • *Entity-Relationship model. The Relational model*

<table>
<tr><td></td><td>

- *Normalization Rules. Codd's 12 rules.*
- *Basic SQL Concepts*
- *SQL Concepts*
- *Advanced SQL concepts: Stored Procedures and Functions*
- *Advanced SQL concepts: Triggers and Transactions*
- *Advanced SQL concepts: SQL Analytics*
- *Advanced SQL concepts: Temporary Tables and CTE's*
- *Database optimization techniques.*
- *Users' role management in DBMS. Dumping in DBMS*
- *NoSQL Concepts and MongoDB*

</td></tr>
<tr><td>Examination forms</td><td>

Exam	*Weight*	*Date*
Final	*40%*	*TBA (to be announced)*
Quizzes	*30%*	*6th week of the semester*
Class activity	*10%*	*every week*
Presentation	*20%*	*TBA (to be announced)*

</td></tr>
<tr><td>Study and examination requirements</td><td>Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (40%)+Before Exam score will remain the same (60%)</td></tr>
<tr><td>Reading list</td><td>

[1] SQL and NoSQL Databases by Andreas Meier and Michael Kaufmann, Springer Vieweg publication, 2019. (main textbook, available in PDF version)

[2] SQL Queries for Mere Mortals by John L.Viescas, Fourth edition, 2018. (main textbook, available in PDF version)

[3] PRACTICAL SQL, A Beginners Guide to Storytelling with Data by Anthony de Barros, No starch press, 2018. (main textbook, available in PDF version)

</td></tr>
</table>

Module designation	***MATH 302 - Linear Algebra***
Semester(s) in which the module is taught	*Year 3, spring semester*
Person responsible for the module	*Assoc. Professor Khanum Jafarova* *BHOS Bibiheybat Campus ROOM 110* *khanum.jafarova@bhos.edu.az*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, seminars, midterms, class tests and activity*
Workload (incl. contact hours, self-study hours)	*Total workload: 150 h = 102h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24 h (2 h /week)* *Seminar: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 8.5 h/ week*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	• *Basic algebra (solving linear equations, factoring, exponents)* • *Elementary matrix operations (addition, multiplication, scalar multiplication)* • *Fundamentals of functions and coordinate geometry* • *Basic understanding of vectors in 2D and 3D space*
Module objectives/intended learning outcomes	• *Students will demonstrate appropriate knowledge in operations with matrices, they will be able to solve the systems of equations by using Gaussian elimination method, by Cramer's rule and with the help of the inverse matrix, to solve application problems, to calculate the eigenvalues and their corresponding eigenvectors.* • *Students will have strong mathematical reasoning and problem solving skills and apply these skills to the solution of theoretical and applied problems in engineering.* • *Students will demonstrate a comprehension of technology by understanding how things work on a fundamental level.*
Content	• *Systems of Linear Equations and Gaussian Elimination* • *Matrices and Basic Matrix Operations* • *Matrix Forms, Rank, and Consistency of Systems* • *Determinants and Their Properties* • *Cramer's Rule and Inverse Matrix Method* • *Applications of Linear Systems in Real-Life Problems* • *Vector Spaces, Subspaces, and Linear Independence* • *Basis, Dimension, and Gram-Schmidt Orthogonalization* • *Linear Transformations and Matrix Representations* • *Algebra of Linear Operators and Change of Basis* • *Eigenvalues and Eigenvectors* • *Diagonalization of Matrices*
	Exam ***Weight*** ***Date***

Examination forms	*Final*	*70%*	*TBA (to be announced)*
	Midterm	*30%*	*6th week of the semester*
Study and examination requirements	*Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (70%)+Before Exam score will remain the same (30%)*		
Reading list	*[1] Stroud K.A. Engineering mathematics; with additions by Dexter J. Booth, 5th edition, Industrial Press, Inc. New York, 2001(available in BHOS library)* *[2] Croft A., Davison R. Mathematics for Engineers , 3rd edition, 2008* *[3] Ron Larson, David C. Falvo, Elementary Linear Algebra, 2009*		

Module designation	***IS 302 - Web programming***
Semester(s) in which the module is taught	*Year 3, spring semester*
Person responsible for the module	*Assoc. Prof. Mahammad Sharifov* *BHOS Bibiheybat Campus ROOM 412* *mahammad.sharifov@bhos.edu.az* *99412 5210000 ext. 33237*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, laboratory work, class tests and activity*
Workload (incl. contact hours, self-study hours)	*Total workload: 150 h = 102h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24 h (2 h /week)* *Laboratory: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 8.5 h/ week*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	• *Basic programming in Java (variables, loops, conditionals, methods, OOP concepts)* • *Fundamentals of HTML, CSS, and JavaScript* • *Basic understanding of web concepts (HTTP/HTTPS, client-server model)* • *Familiarity with databases and SQL*
Module objectives/intended learning outcomes	• *Develop dynamic web applications using Java Servlets, JSP, and JavaScript.* • *Understand and apply security best practices to protect web applications.* • *Identify, exploit, and mitigate common web vulnerabilities.* • *Perform security assessments on web applications using industry tools.* • *Secure RESTful APIs using authentication techniques such as OAuth2 and JWT.* • *Analyse and assess Web application security using tools, testing methods, and cryptographic practices to identify vulnerabilities, ensure secure sessions, communicate findings, and adapt to emerging threats and technologies.*

<table>
<tr><td>Content</td><td>

- *Introduction to Web Programming with Java and Frontend Basics*
- *Web Architecture and Protocols (HTTP/HTTPS)*
- *Java in Web Development (Servlets, JSP)*
- *HTML5, CSS3, and JavaScript Fundamentals*
- *Frontend–Backend Interaction and Form Handling*
- *Dynamic Web Pages with Servlets and JSP*
- *Web Application Security and OWASP Top 10*
- *XSS and SQL Injection Prevention with Secure Database Interaction*
- *Secure Session Management and CSRF Protection*
- *Web Application Firewalls and Security Testing Tools*
- *Secure Java Development Practices and HTTPS/SSL/TLS*
- *API Security, Course Review, and Final Project*

</td></tr>
<tr><td>Examination forms</td><td>

Exam	***Weight***	***Date***
Final	*40%*	*TBA (to be announced)*
Quizzes	*15%*	*every 3 week*
Midterm	*20%*	*6th week of the semester*
Laboraty	*25%*	*every week*

</td></tr>
<tr><td>Study and examination requirements</td><td>Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure, the student can also be given a chance to retake the exam. Resit Exam score (40%) +Before Exam score will remain the same (60%)</td></tr>
<tr><td>Reading list</td><td>

[1] "Core Servlets and JavaServer Pages" by Marty Hall.

[2] MDN Web Docs (online resource).

[3] Pro JSP by Apress.

[4] OWASP (online resource).

[5] The Web Application Hacker's Handbook" by Dafydd Stuttard.

[6] "RESTful Java with JAX-RS" by Bill Burke

</td></tr>
</table>

Module designation	***IS 304 - Cloud Computing***
Semester(s) in which the module is taught	*Year 3, spring semester*
Person responsible for the module	*Lecturer Nihad Alili* *BHOS Bibiheybat Campus ROOM 420* *nihad.elili@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, laboratory work, class tests and activity*
Workload (incl. contact hours, self-study hours)	*Total workload: 150 h = 102h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24 h (2 h /week)* *Laboratory: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 8.5 h/ week*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	• *Basic computer networking concepts (IP addressing, DNS, protocols)* • *Fundamentals of operating systems and virtualization* • *Basic programming and scripting (Python, Bash, or similar)* • *Understanding of databases and storage concepts* • *Basic knowledge of security principles and access control*
Module objectives/intended learning outcomes	• *Explain fundamental cloud concepts and terminology (IaaS/PaaS/SaaS, public/private/hybrid/multi-cloud).* • *Compare and justify service and deployment models for given requirements (cost, performance, security, compliance).* • *Set up and configure cloud environments on a major provider (accounts, IAM, VPC/VNet, storage, compute).* • *Apply cloud security controls and compliance measures (IAM/RBAC, KMS, network segmentation, encryption, backups).* • *Optimize workloads for cost and performance using pricing models, autoscaling and right-sizing; report results.* • *Develop, deploy and manage containerized or serverless applications with CI/CD and basic observability.* • *Monitor and automate cloud operations (logging, metrics, alerts, Infrastructure-as-Code).* • *Evaluate emerging cloud trends and adapt solutions accordingly; reflect on sustainability and vendor lock-in.*
Content	• *Introduction to Cloud Computing and Evolution* • *Cloud Service Models (IaaS, PaaS, SaaS)* • *Cloud Deployment Models (Public, Private, Hybrid, Multi-Cloud)* • *Virtualization in Cloud Computing*

	• *Containerization and Kubernetes* • *Cloud Networking and Storage* • *Cloud Security Fundamentals* • *Compliance and Governance in the Cloud* • *Serverless Computing and Cloud-Native Applications* • *Cost Optimization and Pricing Models* • *Cloud Monitoring and Automation* • *Emerging Trends in Cloud Computing*
Examination forms	***Exam*** ***Weight*** ***Date*** *Final* *40%* *TBA (to be announced)* *Quizzes* *20%* *6th week of the semester* *Class activity* *20%* *every week* *Laboratory* *20%* *every week*
Study and examination requirements	*Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (40%)+Before Exam score will remain the same (60%)*
Reading list	*[1] Cloud Computing: Concepts, Technology & Architecture by Thomas Erl, Zaigham Mahmood, and Ricardo Puttini.* *[2] Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS) by Michael J. Kavis.* *[3] Cloud Computing Bible by Barrie Sosinsky.* *[4] Additional materials, articles, and book chapters will be provided by the instructor.*

Module designation	***IS 306 - Network Security***
Semester(s) in which the module is taught	*Year 3, spring semester*
Person responsible for the module	*Assoc. Prof. Asim Namazov* *BHOS Bibiheybat Campus ROOM 420* *asim.namazov@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, laboratory work, project, presentation*
Workload (incl. contact hours, self-study hours)	*Total workload: 150 h = 102h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24 h (2 h /week)* *Laboratory: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 8.5 h/ week*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	• *Fundamental computer networking concepts (OSI/TCP-IP models, IP addressing, routing, switching)* • *Basic understanding of network devices (routers, switches, firewalls)* • *Familiarity with network protocols (DHCP, ARP, NAT, SNMP, SSH, TCP/UDP)* • *Basic knowledge of network security concepts (firewalls, VPNs, ACLs)* • *Hands-on experience with configuring network devices or simulation tools (e.g., Packet Tracer, GNS3)*
Module objectives/intended learning outcomes	• *Explain core network-security concepts and architectures (threats, trust boundaries, segmentation, control planes).* • *Harden network devices (routers/switches) by configuring management security: SSH, AAA (TACACS+/RADIUS), SNMPv3, CDP/LLDP controls, and secure switch ports.* • *Design and implement traffic control with ACLs, NAT/PAT, and L3/L2 security features; justify rules against stated risks.* • *Deploy and troubleshoot site-to-site and remote-access VPNs (GRE, IPsec/IKE), selecting algorithms and modes appropriate to policy.* • *Configure network resilience (VRRP/HSRP) and assess availability/security trade-offs.* • *Secure DHCP and L2 domains (DHCP Snooping, IP Source Guard, ARP Inspection) and verify effectiveness with test traffic.* • *Document and communicate configurations, risk rationales, and test results in a professional report/presentation; collaborate in teams on a small deployment project.* • *Apply security best practice and relevant policy/ethical constraints; reflect on emerging network-security trends (e.g., zero trust).*

<table>
<tr><td>Content</td><td>

Introduction to Network Security
Security Architecture
Securing Network Devices (CDP, SNMP, LLDP, SSH, TACACS, Switch Port Security)
Virtual Private Networks (GRE, IPSEC)
Network Redundancy (VRRP, HSRP)
DHCP Implementation and Security (DHCP Snooping, ARP Inspection)
Midterm Review
Basic IPv4 Access Control Lists (ACLs)
Advanced IPv4 Access Control Lists (ACLs)
Network Address Translation (Static and Dynamic NAT)
Port Address Translation (PAT)
Network Security Best Practices

</td></tr>
<tr><td>Examination forms</td><td>
<table>
<tr><th>Exam</th><th>Weight</th><th>Date</th></tr>
<tr><td>Final</td><td>40%</td><td>TBA (to be announced)</td></tr>
<tr><td>Project</td><td>30%</td><td>7th week of the semester</td></tr>
<tr><td>Laboratory</td><td>30%</td><td>every week</td></tr>
</table>
</td></tr>
<tr><td>Study and examination requirements</td><td>Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (40%)+Before Exam score will remain the same (60%)</td></tr>
<tr><td>Reading list</td><td>

[1] Data Communications and Computer Networks: A Business User's Approach, Seventh Edition Curt M. White, 2014;
[2] Todd Lammle - CCNA Routing and Switching Study Guide – 2013;
[3] James F. Kurose and Keith W. Ross , Computer Networking - A Top-Down Approach Featuring the Internet, 6th Edition , 2012 Addison Wesley;
[4] Odom W. - Cisco CCNA Routing and Switching 200-120 Official Cert Guide Library – 2013
[5] Andrew S. Tanenbaum, Computer Networks, 5-th Edition,. Prentice Hall, 201 [2] Alan S. Morris. Measurement and Instrumentation Principles. Third Edition. Butterworth-Heinemann, 2001.
[6] CCNA 200-301 Official Cert Guide - WENDELL ODOM

</td></tr>
</table>

Module designation	***IS 308 - Cybersecurity Risk Management***
Semester(s) in which the module is taught	*Year 3, spring semester*
Person responsible for the module	*Lecturer Safura Isayeva* *BHOS Bibiheybat Campus ROOM 420* *safura.isayeva@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, seminars, project, presentation*
Workload (incl. contact hours, self-study hours)	*Total workload: 120 h = 72h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24 h (2 h /week)* *Seminar: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 6 h/ week*
Credit points	*4 ECTS*
Required and recommended prerequisites for joining the module	• *Basic understanding of information security concepts (confidentiality, integrity, availability)* • *Familiarity with cybersecurity fundamentals (network security, malware, access control)* • *Knowledge of IT systems and infrastructure (servers, networks, endpoints, cloud services)* • *Awareness of risk management principles and terminology* • *Basic understanding of security frameworks and standards (ISO 27001, NIST)* • *Experience with security assessment tools or methodologies is helpful but not mandatory*
Module objectives/intended learning outcomes	• *Describe key principles and processes of cybersecurity risk management, including governance, compliance, and legal/regulatory issues.* • *Identify and assess threats, vulnerabilities, and risks using both qualitative and quantitative methods.* • *Analyze and select appropriate risk treatment strategies and controls for various cybersecurity contexts.* • *Develop and implement risk monitoring and reporting mechanisms to communicate with stakeholders.* • *Apply risk management frameworks and standards (e.g., ISO 31000, NIST RMF, COBIT) in real-life scenarios.* • *Work in teams on case studies or projects to evaluate cybersecurity risk in organizations and propose mitigation plans.*
Content	• *Introduction to Cybersecurity Risk Management* • *Risk Assessment Methodologies* • *Threat Modeling and Vulnerability Assessment* • *Security Controls and Mitigation Strategies* • *Risk Treatment and Control Implementation*

	• *Legal, Ethical, and Regulatory Considerations* • *Business Continuity and Disaster Recovery Planning* • *Incident Response and Crisis Management* • *Cybersecurity Risk Management Frameworks* • *Emerging Threats and Advanced Persistent Threats* • *Cloud Security and Third-Party Risk Management* • *Risk Communication, Lab Sessions, and Final Project*
Examination forms	***Exam*** ***Weight*** ***Date*** *Final* *60%* *TBA (to be announced)* *Project* *30%* *6th week of the semester* *Assignment* *10%* *every 3 week*
Study and examination requirements	*Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (60%)+Before Exam score will remain the same (40%)*
Reading list	1. *Umesha Nayak, M.Y. Pirbhulal – The InfoSec Handbook: An Introduction to Information Security* 2. *Charles J. Brooks et al. – Cybersecurity Essentials* 3. *Timothy Shimeall, Jonathan Spring – Introduction to Information Security: A Strategic-Based Approach* 4. *Alan Calder – Nine Steps to Success: An ISO 27001 Implementation Overview* 5. *Dejan Kosutic – ISO 27001 in Plain English*

Module designation	***IS 390 - Internship 2***
Semester(s) in which the module is taught	*Year 3, spring semester*
Person responsible for the module	*Supervisors of Information Technology Department* *BHOS Campus, office , 418* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Mandatory* *BSc program in Information security*
Teaching methods	• *Industrial practice at an approved organization.* • *Supervision and feedback from company mentor and university supervisor.* • *Independent study, daily reporting, and presentation preparation.*
Workload (incl. contact hours, self-study hours)	*Contact hours per week 4 hours* *Private study hours per week 11 hours*
Credit points	*6 ECTS*
Required and recommended prerequisites for joining the module	• *Web Programming: basic front-/back-end skills (HTTP, REST, HTML/CSS/JS, one server-side stack).* • *Introduction to Telecommunication: understanding of OSI/TCP-IP, signalling, bandwidth/latency, and basic routing.* • *Cloud Computing: familiarity with IaaS/PaaS/SaaS, virtualization/containers, IAM, and basic deployment pipelines.* • *Database Fundamentals: SQL/NoSQL basics, normalization, transactions, and backup/restore.* • *Network Security: core defensive controls (FW, IDS/IPS, VPN), secure network architecture, logging/monitoring.* • *Cybersecurity Risk Management: risk identification, assessment (qual./quant.), treatment, and reporting (ISO 27005/NIST).* • *Proficiency in technical writing and professional communication; ethical conduct agreement signed.*
Module objectives/intended learning outcomes	• *Apply systems analysis techniques to clarify business/security requirements and trace them to implemented controls.* • *Implement or support secure web features (authn/authz, input validation, secure session/secret handling) and document changes.* • *Configure, harden, and verify network/telecom components (VLANs, routing, VPN, IDS/IPS rules) under supervision.* • *Deploy and operate cloud services with secure IAM, network segmentation, key management, and baseline compliance checks.* • *Design, query, and secure databases (least privilege, encryption/backup, audit trails) and validate data integrity.* • *Perform vulnerability assessment and basic remediation on hosts, networks, web apps, or cloud resources; record evidence.*

	• *Execute risk assessments for assigned assets, prioritize treatments, and communicate residual risk to stakeholders.* • *Contribute to incident response tasks (triage, log collection, chain of custody, lessons learned) following playbooks.* • *Produce professional technical documentation: daily logs, change/maintenance records, risk register entries, and a final report.* • *Demonstrate teamwork, ethics, and professional conduct, meeting deadlines and responding to feedback from mentors.*
Content	• *Requirements capture & process modelling for a security task.* • *Secure web change/task: small feature or fix with code review & OWASP checks.* • *Network/telecom task: VLAN/VPN configuration, logging enablement, basic monitoring dashboard.* • *Cloud task: least-privilege IAM policy, network segmentation or secure deployment pipeline step.* • *Database task: role design, backup/restore test, encryption at rest/field-level encryption validation.* • *Vulnerability assessment & hardening checklist; re-test and evidence collection.* • *Risk assessment & treatment plan for an assigned system/service.* • *Participation in an incident/DR drill or ticket handling; creation of an IR mini-case.* • *Final report & presentation: results, metrics, evidence, and recommendations.*
Examination forms	***Notes:*** ***Total:*** *100%* ***Grading Scale:*** *A (91–100), B (81–90), C (71–80), D (61–70), F (≤60)* - *Each student is assigned an academic supervisor from BHOS and an industrial mentor from the hosting company.* - *Students must maintain daily logs of activities.* - *A final report (approved and signed by the company supervisor) must be submitted to the BHOS academic supervisor within one week after completion.* *Students must present and defend their internship experience before the BHOS Internship Commission.*
Study and examination requirements	• *Stallings, W. (2023). Computer Security: Principles and Practice. Pearson.* • *Tanenbaum, A. & Bos, H. (2021). Modern Operating Systems. Pearson.* • *Forouzan, B. (2022). Data Communications and Networking. McGraw-Hill.* • *Bishop, M. (2019). Introduction to Computer Security. Addison-Wesley.* *NIST SP 800-53 & ISO/IEC 27001 Standards (for workplace reference).*
Required Documentation	*Before starting the internship:* • *Internship Notice and Program* • *Individual Task Sheet* • *Thematic Task assigned by BHOS Department* *After completion:*

	• *Daily Logbook* • *Final Internship Report (signed by enterprise mentor)* • *Reference Letter from the hosting company* • *PowerPoint Presentation for Defense*

Module designation	***IS 401 - Ethical Hacking & Defence***
Semester(s) in which the module is taught	*Year 4, fall semester*
Person responsible for the module	*Lecturer Elvin Abaszada* *BHOS Bibiheybat Campus ROOM 420* *elvin.abaszade@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, laboratory work, project, presentation*
Workload (incl. contact hours, self-study hours)	*Total workload: 150 h = 102h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24 h (2 h /week)* *Laboratory: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 8.5 h/ week*
Credit points	*5 ETCS*
Required and recommended prerequisites for joining the module	• *Fundamental computer networking (TCP/IP, ports, routing, DNS)* • *Operating systems knowledge (Linux and Windows basics, command line)* • *Basic programming/scripting (Python, Bash, or PowerShell)* • *Familiarity with system administration (users, permissions, services)* • *Introductory information security concepts (CIA triad, authentication, encryption)* • *Experience with virtualization and lab environments (VMs, snapshots)* • *Logical problem-solving and basic forensic thinking (log interpretation)*
Module objectives/intended learning outcomes	• *Explain ethical, legal and professional responsibilities in security testing; define test scope, rules of engagement and evidence-handling procedures.* • *Plan a controlled penetration test: scoping, threat modelling, and method selection (reconnaissance → exploitation → post-exploitation → reporting).* • *Perform information gathering and vulnerability discovery using approved tools (e.g., Nmap, Nessus/OpenVAS, Burp/ZAP); validate findings to avoid false positives.* • *Safely reproduce common attack vectors in an isolated lab (e.g., web, client-side, password and misconfiguration attacks) and demonstrate corresponding defensive mitigations.* • *Exploit and contain a selected vulnerability in a controlled environment while documenting commands, artefacts and impact; propose remediation and hardening steps.* • *Analyse logs, packet captures and host/network artefacts to corroborate exploitation evidence and assess residual risk.*

	• *Produce a professional penetration-test report and present results to technical and non-technical audiences, including an executive summary and a remediation roadmap.*
Content	• *Introduction to Ethical Hacking and Defence* • *Information Gathering* • *Vulnerability Scanning* • *Introduction to Web Applications* • *Common Web Application Attacks* • *SQL Injection Attacks* • *Client-Side Attacks* • *Locating Public Exploits* • *Fixing Exploits* • *Antivirus Evasion* • *Password Attacks*
Examination forms	***Exam*** ***Weight*** ***Date*** *Final* *40%* *TBA (to be announced)* *Laboratory* *30%* *At the end of each week* *Project* *30%* *TBA (to be announced)*
Study and examination requirements	*Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (40%) +Before Exam score will remain the same (60%)*
Reading list	1. *Penetration Testing - A hands-on introduction to Hacking* 2. *Hacker Techniques, Tools, and Incident Handling THIRD EDITION Sean-Philip Oriyano | Michael G.Solomon* 3. *The web application hacker's handbook* 4. *https://www.hackthebox.com/*

Module designation	***IS 403 - IT Security Management***
Semester(s) in which the module is taught	*Year 4, fall semester*
Person responsible for the module	*Lecturer Nihad Alili* *BHOS Bibiheybat Campus ROOM 420* *nihad.elili@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, laboratory work, project, presentation*
Workload (incl. contact hours, self-study hours)	*Total workload: 150 h = 102h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24 h (2 h /week)* *Laboratory: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 8.5 h/ week*
Credit points	*5*
Required and recommended prerequisites for joining the module	• *Basic networking concepts (TCP/IP, routing, switches, firewalls)* • *Fundamentals of information security (CIA triad, authentication, encryption)* • *Operating system administration (Windows & Linux basics, user management, services)* • *Understanding of IT governance and organizational IT structure* • *Basic risk management and compliance awareness* • *Introductory knowledge of security monitoring, logs, and incident response*
Module objectives/intended learning outcomes	• *Explain IT security management principles and justify their role within organisational governance and strategy.* • *Identify and evaluate security management frameworks and standards (e.g., ISO/IEC 27001, NIST CSF/RMF, COBIT) and map them to business contexts.* • *Develop, critique, and maintain security policies, standards, and awareness programmes, aligned to risk appetite and compliance needs.* • *Assess compliance requirements and plan audit activities; produce audit checklists and document findings and corrective actions.* • *Analyse SOC operating models and design incident detection/response workflows using KPIs/KRIs and RACI roles.* • *Apply lifecycle approaches to incident response and crisis management (prepare–identify–contain–eradicate–recover–lessons learned) and report post-incident actions.*
Content	• *Introduction to IT Security Management* • *Security Principles & Human Factors* • *Governance and Security Policies* • *Governance Frameworks*

<table>
<tr><td></td><td>

- *Security Program Management*
- *Compliance Standards*
- *Security Audits and Monitoring*
- *Identity and Access Management (IAM)*
- *Security Operations Centers (SOC)*
- *Incident Response Lifecycle*
- *Business Continuity & Disaster Recovery*
- *Integration & Future Trends*

</td></tr>
<tr><td>Examination forms</td><td>

Exam	***Weight***	***Date***
Final	*50%*	*TBA (to be announced)*
Quizzes	*20%*	*every week*
Laboratory	*15%*	*one task per week*
Presentation	*15%*	*every 3 week*

</td></tr>
<tr><td>Study and examination requirements</td><td>Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure, the student can also be given a chance to retake the exam. Resit Exam score (50%) +Before Exam score will remain the same (50%)</td></tr>
<tr><td>Reading list</td><td>

6. *Umesha Nayak, M.Y. Pirbhulal – The InfoSec Handbook: An Introduction to Information Security*
7. *Charles J. Brooks et al. – Cybersecurity Essentials*
8. *Timothy Shimeall, Jonathan Spring – Introduction to Information Security: A Strategic-Based Approach*
9. *Alan Calder – Nine Steps to Success: An ISO 27001 Implementation Overview*
10. *Dejan Kosutic – ISO 27001 in Plain English*

</td></tr>
</table>

Module designation	***IS 405 - Mobile programming***
Semester(s) in which the module is taught	*Year 4, fall semester*
Person responsible for the module	*Assoc.Prof. Mahammad Sharifov* *BHOS Bibiheybat Campus ROOM 412* *mahammad.sharifov@bhos.edu.az* *99412 5210000 ext. 33237*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, laboratory work, project, presentation*
Workload (incl. contact hours, self-study hours)	*Total workload: 150 h = 102h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24 h (2 h /week)* *Laboratory: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 8.5 h/ week*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	• *Programming fundamentals – proficiency in a high-level language (preferably Java or Kotlin)* • *Object-oriented programming (OOP) concepts* • *Basic understanding of Android development or mobile OS concepts* • *XML for UI design and working with layouts* • *Networking basics (HTTP, APIs, client-server communication)* • *Introduction to security principles (encryption, authentication, secure coding)* • *Familiarity with databases and data persistence (SQL/NoSQL, local storage)*
Module objectives/intended learning outcomes	• *Demonstrate the ability to read and write code using the Kotlin programming language.* • *Explain the fundamentals of Android application lifecycle and mobile app architecture.* • *Design and build user interfaces based on UI/UX design principles and requirements for Android.* • *Integrate and use third-party libraries and frameworks for networking, data serialization, and UI enhancements.* • *Configure and apply security protection rules for Android applications.* • *Compare security models of Android and iOS platforms and identify vulnerabilities specific to mobile devices.* • *Analyze mobile network security threats related to GSM, UMTS, and LTE protocols.* • *Apply best practices to mitigate security vulnerabilities in Bluetooth, SMS, and geolocation services.* • *Evaluate security features of VoIP protocols and apply defensive coding strategies to mobile applications.*

<table>
<tr><td>Content</td><td>

Kotlin fundamentals & XML
Android fundamentals
User interface
Recycler view
User interactions, sensors
Async programming
Reactive programming
Data persistency
Networking
Dependency injection
Clean architecture
Introduction to mobile security
Security of GSM (2G), UMTC (3G) and LTE (4G) network
Bluetooth security
Android security model
iOS security model
SMS security
Mobile geolocation
Security of mobile VoIP communications

</td></tr>
<tr><td>Examination forms</td><td>
<table>
<tr><th>Exam</th><th>Weight</th><th>Date</th></tr>
<tr><td>Final</td><td>40%</td><td>TBA (to be announced)</td></tr>
<tr><td>Assigment</td><td>30%</td><td>6th week of the semester</td></tr>
<tr><td>Laboratory</td><td>30%</td><td>every week</td></tr>
</table>
</td></tr>
<tr><td>Study and examination requirements</td><td>Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (40%)+Before Exam score will remain the same (60%)</td></tr>
<tr><td>Reading list</td><td>

Android Apprentice (Fourth Edition): Beginning Android Development with Kotlin, Namrata Bandekar, Darryl Bayliss, Fuad Kamal, et al., Bowker, 2021.
Kotlin Apprentice: Beginning Programming with Kotlin, Irina Galata, Joe Howard, Dick Lucas, Ellen Shapiro, Razeware LLC, 2021
Mobile Application Security, Himanshu Dwivedi, McGraw Hill, 2010
Security of Mobile Communications, Noureddine Boudriga, Auerbach Publications, 2019
Mobile application penetration testing, Vijay Kumar Velu, Packt publishing, 2016

</td></tr>
</table>

Module designation	***IS 408 - Software Engineering***
Semester(s) in which the module is taught	*Year 4, fall semester*
Person responsible for the module	*Lecturer Orkhan Huseynli* *BHOS Bibiheybat Campus ROOM 420* *orkhan.huseynli@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, laboratory work, project, presentation*
Workload (incl. contact hours, self-study hours)	*Total workload: 150 h = 102h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24 h (2 h /week)* *Laboratory: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 8.5 h/ week*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	• *Programming proficiency – solid knowledge of at least one high-level language (Java, Python, or C#)* • *Object-Oriented Programming (OOP) concepts* • *Basic understanding of software development life cycle (SDLC)* • *Foundations of databases and data management* • *Basic knowledge of web or mobile application development* • *Understanding of software testing principles (unit testing, integration testing)* • *Introduction to security concepts (secure coding, authentication, encryption)* • *Familiarity with version control systems (Git, SVN)*
Module objectives/intended learning outcomes	• *Explain core software-engineering concepts and the Secure SDLC (SSDLC), including roles, artefacts and quality attributes.* • *Elicit and specify user and system requirements (use cases/user stories, acceptance criteria) and trace them through design and tests.* • *Design secure software architectures and justify key decisions (patterns, microservices vs. monolith, data & API design, threat modelling).* • *Implement features using secure coding practices and apply code-analysis tools (linting, SAST/DAST, dependency scanning).* • *Plan and execute multi-level testing (unit, integration, system) and produce verifiable test artefacts (coverage, test reports).* • *Set up and operate DevOps/DevSecOps pipelines (build, test, security checks, containerization) and use version control effectively.* • *Deploy and maintain cloud-based or microservice applications; monitor reliability and performance with basic metrics.* • *Demonstrate professional conduct and evaluate legal/ethical/security responsibilities in software engineering.*

	• *Communicate and collaborate in teams to deliver a working product with documentation, demos and a retrospective.*
Content	• *Introduction to principles of secure software engineering.* • *Focus on developing reliable and secure software systems.* • *Coverage of the complete software development lifecycle.* • *Integration of security and privacy in every stage.* • *Application of Agile and Scrum methodologies.* • *Understanding of software architecture and design principles.* • *Development of cloud-based and microservice applications.* • *Practice of secure coding and code analysis.* • *Implementation of comprehensive software testing techniques.* • *Application of DevOps, automation, and version control.* • *Emphasis on professionalism, ethics, and teamwork.* • *Promotion of problem-solving and continuous learning skills.* • *Principles of secure software engineering; SSDLC* • *Requirements engineering (user stories, acceptance criteria, NFRs)* • *Software architecture & design (patterns, APIs, microservices)* • *Cloud-based and microservice development (containers, orchestration basics)* • *Secure coding & code analysis* • *Software testing (unit, integration, system; TDD/BDD basics)*
Examination forms	***Exam*** ***Weight*** ***Date*** *Final* *80%* *TBA (to be announced)* *Quizzes* *10%* *TBA (to be announced)* *Laboratory* *10%* *every week*
Study and examination requirements	*Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (80%)+Before Exam score will remain the same (20%)*
Reading list	*[1] Ian Sommerville, "Software Engineering:, 10th Edition-Pearson, 2016* *[2] Mark Merkow, "Secure, Resilient, and Agile Software Development", 2020* *[3] Olga Filipova, Rui Vilão, "Software Development From A to Z", Apress (2019)*

Module designation	***IS 409 - Machine Learning Essentials***
Semester(s) in which the module is taught	*Year 4, fall semester*
Person responsible for the module	*Lecturer Mirakram Aghalarov* *BHOS Bibiheybat Campus ROOM 420* *mirakram.aghalarov@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, laboratory work, project, presentation*
Workload (incl. contact hours, self-study hours)	*Total workload: 150 h = 102h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24 h (2 h /week)* *Laboratory: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 8.5 h/ week*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	Linear Algebra, Probability and Statistics, Data Mining for Cybersecurity
Module objectives/intended learning outcomes	• *Explain key ML concepts (supervised/unsupervised, bias–variance, overfitting) and compare common algorithms and use-cases.* • *Prepare datasets: ingest, clean, transform, and engineer features; split data and apply appropriate validation schemes.* • *Implement classical ML models (e.g., k-NN, SVM, tree ensembles, logistic/linear regression) and justify model choice for a given task.* • *Use PyTorch (and companion libraries) to build, train, and evaluate neural networks including CNNs and transformers.* • *Evaluate models with suitable metrics (accuracy/F1/AUC, RMSE/MAE), tune hyperparameters, and document experiments reproducibly.* • *Apply ML to cybersecurity contexts (e.g., anomaly/IDS, malware or phishing detection) and assess model robustness and drift.* • *Describe and apply data-ethics, privacy, and security principles (fairness, re-identification risk, secure model deployment) and recommend mitigations.* • *Communicate results via a short report and presentation including visualisations, error analysis, and limitations.*
Content	• *Introduction to Machine learning (deep learning)* • *Understanding Learning* • *Machine Learning Algorithms* • *Introduction to Deep Learning*

	• *Deeper Networks* • *Convolutional Neural Networks* • *Wake-Up Session: Data Ethics and Protection* • *Natural Language Processing* • *Natural Language Processing with transformers* • *End to End DL Pipeline*
Examination forms	***Exam*** ***Weight*** ***Date*** *Final* *50%* *TBA (to be announced)* *Presentation* *30%* *TBA (to be announced)* *Laboraroty* *20%* *every week*
Study and examination requirements	*Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (50%)+Before Exam score will remain the same (50%)*
Reading list	1. *Aurélien Géron – Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow (Practical ML with Python)* 2. *Christopher M. Bishop – Pattern Recognition and Machine Learning (Foundations of ML theory)* 3. *Ian Goodfellow, Yoshua Bengio, Aaron Courville – Deep Learning (Neural networks and deep learning concepts)* 4. *CMU / CyLab Papers & Labs – Machine Learning for Cybersecurity (Case studies, intrusion detection, malware classification)* 5. *NIST Privacy & ML Guidelines – Publications on privacy-preserving ML and secure deployment of ML models* 6. *UNSW Cybersecurity & ML Course Materials – Open-access tutorials and labs on anomaly detection and security analytics*

Module designation	***IS 402 - Database Administration & Security***
Semester(s) in which the module is taught	*Year 4, spring semester*
Person responsible for the module	*Lecturer Faig Nasirli* *BHOS Bibiheybat Campus ROOM 420* *fayg.nasirli@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, laboratory work, project, presentation*
Workload (incl. contact hours, self-study hours)	*Total workload: 150 h = 102h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24 h (2 h /week)* *Laboratory: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 8.5 h/ week*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	• *Basic understanding of Database Fundamentals (tables, queries, relational models)* • *SQL programming skills* • *Knowledge of database design and normalization* • *Familiarity with database management systems (e.g., MySQL, Oracle, MongoDB)* • *Basic concepts of information security and access control*
Module objectives/intended learning outcomes	• *Design and implement access control rules to assign privileges and protect data* • *Implement control rules to secure stored data* • *Implement Virtual Private Database mechanisms* • *Apply auditing and advanced access control models (MAC, DAC, RBAC)* • *Prepare reports and deliver presentations explaining database security concepts effectively*
Content	1. *Course Description and Security Architecture* 2. *Operating System Security Fundamentals* 3. *Administration of Users, Access Control* 4. *Privileges, passwords, roles, Access Control Models* 5. *Discretionary Access Control and Role-based Access Control* 6. *Mandatory Access Control* 7. *Database Application Security Models, SQL injection* 8. *Database Encryption and Masking* 9. *Virtual Private Databases* 10. *Watermarking* 11. *Database backup and disaster recovery planning* 12. *Performance implications of encryption and auditing.*
Examination forms	***Exam*** ***Weight*** ***Date***

	Final	*40%*	*TBA (to be announced)*
	Quizzes	*30%*	*6th week of the semester*
	Laboratory	*30%*	*every week*
Study and examination requirements	*Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (40%)+Before Exam score will remain the same (60%)*		
Reading list	*[1] Database Security Alfred Basta, Melissa Zgola Database and Applications Security: Integrating Information Security and Data Management Bhavani Thuraisingham* *[2] Implementing Database Security and Auditing 1st Edition by Ron Ben Natan* *[3] Database Systems - Concepts, Languages and Architectures Paolo Atzeni, Stefano Ceri, Stefano Paraboschi and Riccardo Torlone*		

Module designation	***IS 404 - Web and Mobile Security***
Semester(s) in which the module is taught	*Year 4, spring semester*
Person responsible for the module	*Assoc. Prof. Mahammad Sharifov* *BHOS Bibiheybat Campus ROOM 420* *mahammad.sharifov@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, laboratory work, project, presentation*
Workload (incl. contact hours, self-study hours)	*Total workload: 120 h = 72h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24 h (2 h /week)* *Laboratory: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 6 h/ week*
Credit points	*4 ECTS*
Required and recommended prerequisites for joining the module	• *Web programming fundamentals (HTML, CSS, JavaScript)* • *Java programming and Java Servlets/JSP basics* • *Database concepts and SQL* • *Understanding of basic networking concepts (HTTP/HTTPS)* • *Basic knowledge of security principles and vulnerabilities (e.g., XSS, SQL Injection)*
Module objectives/intended learning outcomes	• *Develop dynamic, database-driven web applications using Java (Servlets, JSP, JDBC)* • *Integrate frontend (HTML, CSS, JavaScript) with backend components* • *Apply secure coding practices to prevent common web vulnerabilities (XSS, SQL Injection, CSRF)* • *Implement secure authentication, session management, and access controls* • *Protect data and APIs using SSL/TLS, OAuth2, and JWT* • *Use security testing tools and perform vulnerability assessments (OWASP ZAP, Burp Suite)* • *Build, deploy, and present a complete secure web application project*
Content	• *Introduction to Web Programming with Java and Frontend Basics (HTML, CSS, JavaScript)* • *Java Servlets and JSP for Dynamic Web Pages* • *Introduction to Web Application Security* • *Cross-Site Scripting (XSS) and SQL Injection and Secure Database Interaction* • *Secure Session Management and CSRF Protection, Web Application Firewalls (WAF) and Security Tools* • *Secure Development Practices in Java* • *HTTPS, SSL/TLS and Certificate M*

<table>
<tr><td></td><td>

- *API Security and Secure Communication*

</td></tr>
<tr><td>Examination forms</td><td>

Exam	***Weight***	***Date***
Final	*40%*	*TBA (to be announced)*
Quizzes	*15%*	*6th week of the semester*
Laboratory	*25%*	*every week*
Project	*20*	*TBA (to be announced)*

</td></tr>
<tr><td>Study and examination requirements</td><td>Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (40%)+Before Exam score will remain the same (60%)</td></tr>
<tr><td>Reading list</td><td>[1] "Core Servlets and JavaServer Pages" by Marty Hall.
[2] MDN Web Docs (online resource).
[3] Pro JSP by Apress.
[4] OWASP (online resource).
[5] The Web Application Hacker's Handbook" by Dafydd Stuttard.
[6] "RESTful Java with JAX-RS" by Bill Burke</td></tr>
</table>

Module designation	***IS 406 - Introduction to Malware Analysis***
Semester(s) in which the module is taught	*Year 4, spring semester*
Person responsible for the module	*Lecturer Nihad Alili* *BHOS Bibiheybat Campus ROOM 420* *nihad.elili@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, laboratory work, project, presentation*
Workload (incl. contact hours, self-study hours)	*Total workload: 150 h = 102h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24 h (2 h /week)* *Laboratory: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 8.5 h/ week*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	• *Fundamentals of computer security and network security* • *Programming knowledge (e.g., C/C++, Python)* • *Operating system concepts, especially Windows and Linux internals* • *Basic knowledge of assembly language and low-level programming* • *Understanding of debugging and reverse engineering basics* • *Familiarity with virtual machines and sandbox environments*
Module objectives/intended learning outcomes	• *Classify malware families, delivery vectors, and typical TTPs; explain the kill chain and mapping to MITRE ATT&CK.* • *Set up, harden, and operate an isolated malware analysis lab (VM networking, snapshots, tooling, safe handling SOPs).* • *Perform static analysis (hashing, strings, PE/ELF inspection, packer detection, control-flow overview) using disassembly tools.* • *Perform dynamic analysis in sandboxes and with debuggers; trace process, file, registry, and network behaviours.* • *Analyse memory images to detect persistence, injection, hooking and stealth techniques (e.g., DLL injection, API hooking).* • *Identify and bypass common anti-analysis/anti-VM techniques, documenting limitations and counter-measures.* • *Report reproducible findings (IoCs, YARA/Sigma rules, triage notes) and communicate containment/mitigation recommendations.* • *Demonstrate legal, ethical and safety practice in handling malicious code; reflect on responsible disclosure and licensing*
Content	• *Introduction to Malware Analysis*

<table>
<tr><td></td><td>

- *Setting Up a Malware Analysis Lab*
- *Static Analysis*
- *Advanced Static Analysis*
- *Dynamic Analysis*
- *Debugging and Reverse Engineering Basics*
- *Advanced Malware Techniques*
- *Malware Persistence Mechanisms*
- *Ransomware Analysis*
- *Memory Forensics*
- *Case Studies*

</td></tr>
<tr><td>Examination forms</td><td>

Exam	***Weight***	***Date***
Final	*40%*	*TBA (to be announced)*
Quizzes	*30%*	*6th week of the semester*
Laboratory	*30%*	*every week*

</td></tr>
<tr><td>Study and examination requirements</td><td>Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (40%)+Before Exam score will remain the same (60%)</td></tr>
<tr><td>Reading list</td><td>

- ***Alexey Kleymenov, Amr Thabet*** - *Mastering Malware Analysis (2019)*
- ***Michael Sikorski, Andrew Honig*** - *Practical Malware Analysis -No Starch Press (2012)*
- ***Monnappa K. A.*** - *Learning Malware Analysis - Packt Publishing (2018)*
- ***Reginald Wong*** - *Mastering Reverse Engineering*

</td></tr>
</table>

Module designation	***IS 408 - Vulnerability Assessment & Penetration Testing***
Semester(s) in which the module is taught	*Year 4, spring semester*
Person responsible for the module	*Lecturer Elvin Abaszade* *BHOS Bibiheybat Campus ROOM 420* *elvin.abaszade@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, laboratory work, project, presentation*
Workload (incl. contact hours, self-study hours)	*Total workload: 150 h = 102h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24 h (2 h /week)* *Laboratory: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 8.5 h/ week*
Credit points	*5 ETCS*
Required and recommended prerequisites for joining the module	• *Fundamentals of computer and network security* • *Operating system knowledge (Windows and Linux)* • *Basic networking concepts and protocols (TCP/IP, DNS, HTTP/S)* • *Programming/scripting skills (Python, Bash, or PowerShell)* • *Familiarity with web technologies (HTML, CSS, JavaScript)* • *Understanding of authentication, access control, and encryption concepts*
Module objectives/intended learning outcomes	• *Plan and execute penetration tests using standard methodologies.* • *Discover targets, services, and network topology through reconnaissance.* • *Identify open ports, running services, and fingerprint operating systems.* • *Conduct automated vulnerability scans and interpret results effectively.* • *Assess security of network devices, Windows, and Linux systems.* • *Perform web application security testing and identify vulnerabilities.* • *Document findings and provide actionable remediation recommendations.* • *Evaluate organizational security posture and support compliance and incident response.*
Content	• *Intro & Pen Test Methodologies* • *Content Discovery, Authentication, and Session Testing* • *Port Redirection and SSH Tunneling* • *Vulnerability Scanning* • *Web Application Attacks* • *The Metasploit Framework* • *Wireless Network attacks* • *Post Exploitation* • *Privilege Escalation in Linux*

	• *Privilege Escalation in Windows* • *Active Directory and its attacks*
Examination forms	***Exam*** ***Weight*** ***Date*** *Final* *40%* *TBA (to be announced)* *Laboratory* *40%* *every week* *Presentation* *20%* *TBA (to be announced)*
Study and examination requirements	*Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (60%)+Before Exam score will remain the same (40%)*
Reading list	*[1] Penetration Testing With Kali Linux Authors: Offensive Security* *[2] Penetration Testing: A Hands-On Introduction to Hacking 1st Edition by Georgia Weidman* *[3] Cybersecurity – Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics by Yuri Diogenes (Author), Erdal Ozkaya* *[4] Buffer Overflow Attacks: Detect, Exploit, Prevent 1st Edition by James C. Foster (Author), Vitaly Osipov (Author), Nish Bhalla (Author)* *[5] Hands-On Penetration Testing on Windows: Unleash Kali Linux, PowerShell, and Windows debugging tools for security testing and analysis by Phil Bramwel*

Module designation	***IS 490 - Internship 3***
Semester(s) in which the module is taught	*Year 4, spring semester*
Person responsible for the module	*Supervisors of Information Technology Department* *BHOS Campus, office , 418* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Mandatory* *BSc program in Information security*
Teaching methods	• *Industrial practice at an approved organization.* • *Supervision and feedback from company mentor and university supervisor.* • *Independent study, daily reporting, and presentation preparation.*
Workload (incl. contact hours, self-study hours)	*Contact hours per week 4 hours* *Private study hours per week 11 hours*
Credit points	*6 ETCS*
Required and recommended prerequisites for joining the module	• *Completion of core cybersecurity modules including Network Security, Operating Systems Security, and Incident Response and Digital Forensics.* • *Basic proficiency in Python or PowerShell for automation and scripting.* • *Familiarity with SIEM platforms, threat intelligence tools, and penetration testing methodologies.* • *Foundational knowledge of risk management frameworks (e.g., ISO/IEC 27001, NIST).* • *Understanding of organizational security policies, compliance, and reporting structures.*
Module objectives/intended learning outcomes	• *Apply theoretical and practical cybersecurity knowledge in real-world organizational settings.* • *Perform security assessments, analyze vulnerabilities, and document mitigation strategies.* • *Demonstrate the ability to use industry-standard tools such as SIEMs, IDS/IPS systems, and vulnerability scanners.* • *Develop, execute, and document incident response procedures aligned with SOC workflows.* • *Integrate risk management and policy compliance principles into daily security operations.* • *Collaborate effectively in multidisciplinary teams to deliver security projects and maintain documentation to professional standards.* • *Present findings and communicate technical details clearly through written reports and oral presentations to both technical and non-technical audiences.* • *Reflect critically on ethical, legal, and professional responsibilities in cybersecurity practice.*

Content	• *Overview of Industrial and Research-based Security Practices* • *Security Operations Center (SOC) Structure and Workflow* • *Threat Monitoring, Detection, and Reporting Procedures* • *Vulnerability Management and Penetration Testing Cycles* • *Risk Assessment and Governance in Enterprise Environments* • *Cybersecurity Incident Response and Forensic Documentation* • *Compliance and Regulatory Frameworks (ISO/IEC 27001, NIST SP 800-53)* • *Security Project Management and Communication with Stakeholders* • *Internship/Project Reporting Guidelines and Final Presentation Preparation*
Examination forms	***Notes:*** ***Total:*** *100%* ***Grading Scale:*** *A (91–100), B (81–90), C (71–80), D (61–70), F (≤60)* - *Each student is assigned an academic supervisor from BHOS and an industrial mentor from the hosting company.* - *Students must maintain daily logs of activities.* - *A final report (approved and signed by the company supervisor) must be submitted to the BHOS academic supervisor within one week after completion.* *Students must present and defend their internship experience before the BHOS Internship Commission.*
Study and examination requirements	• *Stallings, W. (2023). Computer Security: Principles and Practice. Pearson.* • *Tanenbaum, A. & Bos, H. (2021). Modern Operating Systems. Pearson.* • *Forouzan, B. (2022). Data Communications and Networking. McGraw-Hill.* • *Bishop, M. (2019). Introduction to Computer Security. Addison-Wesley.* *NIST SP 800-53 & ISO/IEC 27001 Standards (for workplace reference).*
Required Documentation	*Before starting the internship:* • *Internship Notice and Program* • *Individual Task Sheet* • *Thematic Task assigned by BHOS Department* *After completion:* • *Daily Logbook* • *Final Internship Report (signed by enterprise mentor)* • *Reference Letter from the hosting company* • *PowerPoint Presentation for Defense*

Module designation	***IS 501 - IoT Security***
Semester(s) in which the module is taught	*Year 5, fall semester*
Person responsible for the module	*Lecturer Elshan Rahimov* *BHOS Bibiheybat Campus ROOM 420* *elshan.rahimov@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, laboratory work, presentation*
Workload (incl. contact hours, self-study hours)	*Total workload: 180 h = 132h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24 h (2 h /week)* *Laboratory: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 11 h/ week*
Credit points	*6 ETCS*
Required and recommended prerequisites for joining the module	• *Fundamentals of computer networks and Internet protocols* • *Basic programming skills (Python, C/C++, or similar)* • *Knowledge of embedded systems and microcontrollers* • *Understanding of operating systems and hardware components* • *Basic cybersecurity concepts, including access control, encryption, and secure communication* • *Familiarity with mobile technologies and wireless communication standards (e.g., Wi-Fi, Bluetooth, GSM)*
Module objectives/intended learning outcomes	• *Explain the IoT stack (device–edge–cloud), common protocols (MQTT, CoAP, BLE, Zigbee, Wi-Fi), and typical threats across layers.* • *Model and prioritise risks for IoT systems using an appropriate method (e.g., STRIDE/LINDDUN) with impact/likelihood scoring.* • *Design secure device and gateway architectures (secure boot, HW roots of trust/TPM, firmware signing, key provisioning, update/rollback strategy).* • *Implement and configure secure communication (TLS/DTLS, WPA2/3, BLE pairing/bonding) and access control for devices, APIs, and cloud back-ends.* • *Assess firmware and device security (enumerate interfaces such as UART/JTAG, extract/inspect firmware, identify hard-coded secrets and weak crypto).* • *Instrument and operate an IoT security lab environment (device simulators, traffic capture, fuzzing/basic exploitation for protocol robustness).* • *Demonstrate compliance and ethical practice: privacy-by-design for IoT data, alignment with NISTIR 8259A, ENISA and OWASP IoT Top-10; communicate findings to technical and non-technical stakeholders.*

	• *Reflect on emerging trends (IoT identity at scale, SBOMs, secure update ecosystems, edge AI safety) and outline a personal learning plan*
Content	• *IoT - Introduction, Definitions and Properties* • *IoT main directions and how to apply* • *Creation of IoT process on the base of mobile Technologies* • *Learning of security items in IoT process* • *Applying of Security methods in IoT process* • *Researching of operating security mechanisms in real-time woring IoT process* • *IoT in a various life areas* • *IoT and Telematics devices* • *Appliyng of different security strategies to various IoT projects* • *Data exchange in IoT and Mobile Technologies in IoT* • *IoT device Security*
Examination forms	***Exam*** ***Weight*** ***Date*** *Final* *50%* *TBA (to be announced)* *Laboratory* *40%* *every week* *Presentation* *10%* *TBA (to be announced)*
Study and examination requirements	*Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure, the student can also be given a chance to retake the exam. Resit Exam score (50%) +Before Exam score will remain the same (50%)*
Reading list	*[1] IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing,DavidHanis, Cisco Press; 1 edition, 2017, 575 pages.* *[2] Introduction to IoT Security, Anca D. Jurcut, Pasika Ranaweera, Lina Xu, University College Dublin, Ireland, 2021, 37 pages.* *[3]Building the Internet of Things: Implement New Business Models, Disrupt Competitors, Transform Your Industry,MaciejKranz, Wiley Publishers, 2016, 272 pages.* *[4]Precision: Principles, Practices and Solutions for the Internet of Things, Timothy Chou, lulu.com, 2016,312 pages.* *[5] IoT Security for dummies, Lawrence Miller, John Willey & Sons Ltd, 2016, 53 pages.* *[6] Enforcing Security Mechanisms in the IP-Based Internet of Thing: An Algorithmic Overview, Simone Cirani, Gianluigi Ferrari, and Luca Veltri, Algorithms 2013, N6, pp.197-226.*

Module designation	***IS 503 - Legal Issues in Information Security***
Semester(s) in which the module is taught	*Year 5, fall semester*
Person responsible for the module	*Lecturer Nigar Guliyeva* *BHOS Bibiheybat Campus ROOM 420* *nigar.guliyeva@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, laboratory work, presentation*
Workload (incl. contact hours, self-study hours)	*Total workload: 180 h = 132h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24 h (2 h /week)* *Laboratory: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 11 h/ week*
Credit points	*6 ECTS*
Required and recommended prerequisites for joining the module	• *Basic understanding of information security and cybersecurity concepts* • *Familiarity with digital technologies, networks, and data processing* • *General knowledge of computer systems, software, and Internet applications* • *Awareness of ethical issues in technology and data privacy* • *Basic understanding of national and international regulatory environments (helpful but not mandatory)*
Module objectives/intended learning outcomes	• *Explain the main international and national legal frameworks governing personal data, cybersecurity, electronic identity/signature, e-commerce, IP, and cybercrime in Azerbaijan and comparable jurisdictions.* • *Interpret and apply data-protection obligations (lawful basis, rights of data subjects, DPIA, cross-border transfer restrictions) to concrete technical scenarios.* • *Analyse platform, AI, and algorithmic-accountability issues (automated decision-making, transparency, bias, human-rights impacts) and formulate policy options.* • *Identify and compare obligations for critical-infrastructure protection, incident reporting, and cybercrime enforcement; outline lawful evidence handling.* • *Draft and critique core governance artefacts (privacy notice, consent language, security policy, acceptable-use policy, ToS/DPAs) for clarity and compliance.* • *Construct legal arguments and present case-based conclusions in written and oral formats to specialist and non-specialist audiences.*

	• *Evaluate ethical trade-offs (security vs. privacy, free expression, competition, consumer protection) and recommend defensible, risk-based decisions.* • *Plan ongoing professional development by tracking evolving standards (AI governance, children's data, cross-border data, platform regulation) and mapping learning needs.*
Content	• *Introduction to Internet Law and Data Protection* • *The Role of Big Tech in the Digital Society* • *Digital Identity, E-Governance & Electronic Signatures* • *Artificial Intelligence and the Law* • *E-Commerce and Consumer Protection Law* • *Intellectual Property in the Cyber Domain* • *Algorithms, Ethics, and Human Rights* • *National Cybersecurity & Critical Infrastructure Protection* • *Cybercrime and Global Threats* • *National Legal Framework – Cyber Law in AR* • *Legal Innovation, Policy Evaluation, and Trends*
Examination forms	***Exam*** ***Weight*** ***Date*** *Final* *50%* *TBA (to be announced)* *Quizzes* *30%* *at the end of each topic* *Presentation* *20%* *TBA (to be announced)*
Study and examination requirements	*Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (50%)+Before Exam score will remain the same (50%)*
Reading list	1. *AR National Strategy on AI* 2. *The Law of the Republic of Azerbaijan "On personal data" #998-IIIQ dated May 11, 2010.* 3. *The Law of the Republic of Azerbaijan "On biometric information" #651-IIIQ dated June 13, 2008.* 4. *The Law of the Republic of Azerbaijan "On access to information" #1024-IIQ dated September 30, 2005.* 5. *"Law on Information, Informatization, and Protection of Information" #460-IQ dated April 1998,* 6. *Law "On Electronic Signature and Electronic Document" # 602-IIQ dated March 9 2004* 7. *"Rules for ensuring the security of critical information infrastructure in the Republic of Azerbaijan" dated July 19, 2023* 8. *"Requirements for ensuring information security in entities whose activities are controlled in financial markets" dated March 2024*

Module designation	***IS 505 - Forensic Science***
Semester(s) in which the module is taught	*Year 5, fall semester*
Person responsible for the module	*Assoc.Prof. Gunay Abdiyeva-Aliyeva* *BHOS Bibiheybat Campus ROOM 420* *gunay.abdiyeva@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, laboratory work, presentation*
Workload (incl. contact hours, self-study hours)	*Total workload: 180 h = 132h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24 h (2 h /week)* *Laboratory: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 11 h/ week*
Credit points	*6 ECTS*
Required and recommended prerequisites for joining the module	• *Basic understanding of computer systems, operating systems (Windows, Linux, macOS)* • *Fundamentals of networking and network protocols* • *Knowledge of information security and cybersecurity principles* • *Familiarity with malware, threats, and cybercrime concepts* • *Basic skills in handling digital data and using security tools*
Module objectives/intended learning outcomes	• *Explain how to prepare a digital forensics investigation using a systematic methodology.* • *Analyze the impact of evolving technologies on cybercrime patterns.* • *Determine and evaluate what data to collect and analyze for evidence.* • *Describe and apply standard procedures for forensic acquisition and analysis.* • *Utilize diverse computer forensic tools to examine digital crime scenes.* • *Apply modern techniques for data recovery, duplication, and evidence preservation.* • *Integrate ethical and legal perspectives in forensic practice and reporting.*
Content	• *Computer Forensics Fundamentals* • *Digital Forensic Investigation Process and Methodology* • *Understanding Storage Media (HDD, SSD) and File Systems* • *Data Acquisition and Duplication Techniques* • *Anti-Forensics Detection and Countermeasures* • *Windows, Linux, and Mac Forensics* • *Network Forensics and Web Attack Analysis* • *Dark Web and Email Forensics*

<table>
<tr><td></td><td>

- *Malware Forensics and Incident Correlation*
- *Reporting and Evidence Documentation*

</td></tr>
<tr><td>Examination forms</td><td>

Exam	***Weight***	***Date***
Final	*40%*	*TBA (to be announced)*
Laboratory	*30%*	*every week*
Presentation	*30%*	*TBA (to be announced)*

</td></tr>
<tr><td>Study and examination requirements</td><td>*Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (40%)+Before Exam score will remain the same (60%)*</td></tr>
<tr><td>Reading list</td><td>

[1] Digital Forensics Essentials D|FE Version 1. Professional Series. EC-Council.

[2] Nelson, B., Phillips, A., & Steuart, C. (2016). Guide to Computer Forensics and Investigations (5th ed.). Boston, MA: CENGAGE Learning. ISBN 1-285-06003-2, 978- 1-285-06003-3.

[3] Oettinger, W. Learn Computer Forensics: Your one-stop guide to searching, analyzing, acquiring, and securing digital evidence, 2nd Edition

[4] Gogolin, G. (2021) Digital Forensics Explained (Kindle Edition).

</td></tr>
</table>

Module designation	***IS 507 - Blockchain***
Semester(s) in which the module is taught	*Year 5, fall semester*
Person responsible for the module	*Lecturer Nihad Alili* *BHOS Bibiheybat Campus ROOM 420* *nihad.elili@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, laboratory work, presentation*
Workload (incl. contact hours, self-study hours)	*Total workload: 180 h = 132h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24 h (2 h /week)* *Laboratory: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 11 h/ week*
Credit points	*6 ECTS*
Required and recommended prerequisites for joining the module	• *Fundamentals of computer science and programming (variables, functions, control flow)* • *Basic discrete mathematics (sets, functions, logic)* • *Data structures and algorithms (arrays, lists, hash maps; asymptotic complexity basics)* • *Introductory cryptography and security principles (hashes, symmetric/asymmetric crypto, digital signatures)*
Module objectives/intended learning outcomes	• *Explain blockchain structure, components, and types.* • *Apply cryptography to secure blockchain transactions.* • *Develop and deploy smart contracts on Ethereum.* • *Analyze blockchain consensus algorithms (Proof-of-Work, Proof-of-Stake, etc.).* • *Identify and mitigate security risks in blockchain systems.* • *Implement blockchain applications for secure data and identity management.* • *Use blockchain development tools like Solidity, Truffle, and Hyperledger.* • *Evaluate real-world blockchain case studies in cybersecurity contexts*
Content	• *Introduction to Blockchain* • *Cryptography in Blockchain* • *Blockchain Architecture* • *Consensus Mechanisms* • *Cryptocurrencies & Bitcoin* • *Ethereum & Smart Contracts* • *Advanced Smart Contracts* • *Blockchain Security* • *Hyperledger & Enterprise Blockchain* • *Blockchain in Cybersecurity*

	• *Blockchain Applications*
Examination forms	***Exam*** ***Weight*** ***Date*** *Final* *40%* *TBA (to be announced)* *Laboratory* *30%* *every week* *Presentation* *30%* *TBA (to be announced)*
Study and examination requirements	*Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (40%)+Before Exam score will remain the same (60%)*
Reading list	• *Mastering Bitcoin by Andreas Antonopoulos* • *Blockchain Basics by Daniel Drescher* • *Mastering Ethereum by Andreas Antonopoulos & Gavin Wood*

Module designation	***MACD 504 - Safety, Health and civil Defense***
Semester(s) in which the module is taught	*Year 5, spring semester*
Person responsible for the module	*Professor Kanan Yusifzada* *BHOS Bibiheybat Campus ROOM 420* *kanan.yusif-zada@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lecture, Practical work*
Workload (incl. contact hours, self-study hours)	*Total workload: 150 h = 126h extracurricular hours + 24h classroom* ***Classroom hours**:* *Lecture: 12 h (1 h /week)* *Laboratory: 12 h (1 h / week)* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 10.5 h/ week*
Credit points	*5 ETCS*
Required and recommended prerequisites for joining the module	• *ESH 202 – Electrical Safety*
Module objectives/intended learning outcomes	*By the end of this course, students will be able to:* • *Explain the fundamental concepts of civil defence, emergency preparedness, and disaster management systems.* • *Identify and assess potential natural and human-made hazards relevant to engineering and industrial environments.* • *Apply basic first aid and medical assistance techniques in case of accidents or emergency situations.* • *Demonstrate knowledge of safety procedures, evacuation plans, and protective measures for individuals and workplaces.* • *Analyze the roles and responsibilities of engineers and technical specialists in maintaining occupational safety and public protection.* • *Promote a culture of safety, awareness, and responsibility in professional and societal contexts.*
Content	*In teaching civil defense: classification of urgent and emergency circumstances in war and peaceful period, general questions of civil defense, impact of urgent and emergency circumstances are explained. In urgent and emergency circumstances, protection methods of population, main objectives of civil defense medical aid, provision of pre-hospital medical aid in injuries, carrying out anti-epidemic and sanitary and hygienic measures, rules of providing treatment and preventive aid to population.*
Examination forms	***Exam*** ***Weight*** ***Date***

	Final	*60%*	*TBA (to be announced)*
	Quiz	*20%*	*every week*
	Presentation	*20%*	*TBA (to be announced)*
Study and examination requirements	*Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (60%)+Before Exam score will remain the same (40%)*		
Reading list	***Teaching materials**:* *Presentations: Lecture notes and presentations (www.lms.bhos.edu.az)* ***Textbooks:*** • *http://www.ipieca.org/publication/managing-health-field-operations-oil-and-gas-activities* • *Emergency safety and first aid handbook. http://www.ddm.gov.bt/download/Emergency* • *Prof. Dr. K.Yusif-zada. Semi-Public Hospital Management* ***Software:** -* *For class presentations and discussions, the student should utilize journal and internet materials. Moreover, the course does not limit the use of learning materials available at BHOS library.*		

Module designation	***IS 599– Final Project (Graduation work)***
Semester(s) in which the module is taught	*Year 5, Spring semester*
Person responsible for the module	Supervisors of Information Technology Department *BHOS Campus, office , 418* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Compulsory* *BSc program in Information security*
Teaching methods	- *Supervised individual or team project work* - *Weekly or bi-weekly progress meetings with supervisor* - *Independent research, design, and implementation* - *Lab sessions for hands-on development and testing* - *Peer review and self-assessment activities*
Workload (incl. contact hours, self-study hours)	*Total workload: 300 h = 300 h extracurricular hours* ***Classroom hours****:* - ***Contact hours:*** *Project preparation, consultation, self-study = 25 h/ week*
Credit points	*10 ECTS*
Required and recommended prerequisites for joining the module	• *Completion of all core Information Security courses* • *Programming and software development skills* • *Knowledge of relevant tools and platforms in chosen domain* • *Approval of project proposal by supervisor*
Module objectives/intended learning outcomes	***Module Description:*** *The Final Project represents the culmination of the Information Technology bachelor program, where students apply theoretical knowledge and technical competencies to solve a practical or research-oriented IT problem. Students will work individually or in teams to design, develop, test, and document an information system, application, or infrastructure solution under faculty supervision. Projects may involve web and cloud platforms, data analytics, cybersecurity, artificial intelligence, or enterprise information systems.* ***Module Objectives:*** *By the end of this module, students will be able to:* 1. *Apply IT and engineering knowledge to identify, design, and solve complex digital problems.* 2. *Conduct requirement analysis, system modeling, and technical research.* 3. *Integrate hardware, software, and network components into a unified system.* 4. *Implement and validate solutions using modern IT tools, frameworks, and environments.*

	5. *Communicate technical results effectively through written documentation and oral presentations.* 6. *Demonstrate project planning, collaboration, and quality assurance skills.* ***Learning Outcomes:*** *Upon successful completion of the Capstone Project, students will be able to:* 1. *Define project objectives and technical requirements aligned with organizational or research needs.* 2. *Design and develop scalable, secure, and efficient IT systems or applications.* 3. *Apply IT project management principles, including version control, task scheduling, and risk mitigation.* 4. *Evaluate performance, usability, and security aspects of implemented solutions.* 5. *Document design processes, methodologies, and test results in a professional technical report.* 6. *Present findings effectively to both technical and non-technical audiences.* 7. *Exhibit problem-solving, critical thinking, and teamwork skills.*
Content	***Topics / Activities*** *1* *Project Proposal – Identify problem, objectives, methodology, and expected outcomes.* *2* *Requirements Analysis – Gather and document functional and non-functional requirements.* *3* *System Design – Develop architecture, UML diagrams, data models, or hardware schematics.* *4* *Implementation – Develop software, integrate systems, or prototype hardware solution.* *5* *Testing & Validation – Unit testing, integration testing, system testing, performance evaluation.* *6* *Documentation – Prepare technical report detailing objectives, methodology, design, implementation, results, and conclusions.* *7* *Presentation & Defense – Demonstrate the project and defend methodology and results before a faculty panel.*
Examination forms	*Supervisor Review* *33%* *Final Technical Report/ Turnitin* *33%* *Final Presentation and Defense* *33%*
Study and examination requirements	***Notes:*** • *Students are required to submit progress reports at designated milestones.* • *The project topic must be approved by the faculty supervisor before implementation.* • *Collaboration with industry or research labs is encouraged for real-world exposure.*
Reading list	***Teaching materials****:*

	Textbooks: - *Depends on the scope of Project* ***Software:*** - *Depends on the scope of Project* *For class presentations and discussions, the student should utilize journal and internet materials. Moreover, the course does not limit the use of learning materials available at BHOS library.*

Elective courses

Module designation	***IS 411 - Realiability Theory***
Semester(s) in which the module is taught	*Year 4, fall semester*
Person responsible for the module	*Lecturer Orkhan Huseynli* *BHOS Bibiheybat Campus ROOM 420* *orkhan.huseynli@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Elective*
Teaching methods	*Lectures, laboratory work, assignments, quizzes*
Workload (incl. contact hours, self-study hours)	*Total workload: 150 h = 102h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24h (2 h /week)* *Laboratory: 24h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 8.5 h/ week*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	• *Basic probability theory: random variables, common distributions, expectation/variance.* • *Basic statistics: point estimation, confidence intervals, hypothesis testing.* • *Elementary calculus: differentiation and integration (including exponential/log functions).* • *Linear algebra essentials: vectors/matrices, eigenvalues (for Markov/transition analysis).*
Module objectives/intended learning outcomes	• *Define and interpret key reliability metrics (reliability function, hazard rate, MTTF, availability).* • *Describe major life-time distributions (Exponential, Weibull, Log-normal, Gamma) and their ageing properties.* • *Analyse reliability of simple systems (series, parallel, k-out-of-n, coherent systems).* • *Estimate distribution parameters and reliability measures using life-time data (including censored data).* • *Model repairable systems and calculate availability using renewal and Markov processes.* • *Apply reliability block diagrams and fault-tree methods to system reliability modelling.* • *Evaluate dependence effects, common-cause failures, and their influence on system reliability.* • *Develop maintenance and replacement strategies based on reliability and cost trade-offs.* • *Communicate reliability analysis results and understand their implications in engineering design and maintenance.*

Content	• *Introduction to reliability theory: basic concepts, measures, and real-world applications* • *Review of probability concepts and life-time distributions (Exponential, Weibull, Log-normal, Gamma)* • *Ageing properties, hazard functions, and the bathtub curve* • *System reliability structures: series, parallel, and k-out-of-n systems* • *Coherent systems, minimal path and cut sets, and component importance measures* • *Parameter estimation and reliability data analysis (complete and censored data)* • *Repairable systems and availability models using renewal and Markov processes* • *Reliability block diagrams, fault-tree and event-tree analysis* • *Dependence between components and common-cause failures* • *Maintenance and replacement policies: preventive, corrective, and optimal strategies* • *Software reliability, accelerated life testing, and reliability growth models* • *Case studies, project presentations, and course review*
Examination forms	***Exam*** ***Weight*** ***Date*** *Final* *60%* *TBA (to be announced)* *Quiz* *20%* *every week* *Assignment* *20%* *TBA (to be announced)*
Study and examination requirements	*Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (60%)+Before Exam score will remain the same (40%)*
Reading list	• Rausand, M., Barros, A., & Hoyland, A. System Reliability Theory: Models, Statistical Methods, and Applications (3rd ed.). Wiley, 2021. • Rao, S. S. Reliability Engineering. Pearson. • Leemis, L. Reliability: Probabilistic Models and Statistical Methods. Prentice Hall.

Module designation	***IS 413 - Software Fault Tollerance***
Semester(s) in which the module is taught	*Year 4, fall semester*
Person responsible for the module	*Lecturer Orkhan Huseynli* *BHOS Bibiheybat Campus ROOM 420* *orkhan.huseynli@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Elective*
Teaching methods	*Lectures, presentation*
Workload (incl. contact hours, self-study hours)	*Total workload: 150 h = 102h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24h (2 h /week)* *Laboratory: 24h (2 h / week)s* ***Contact hours:*** *Examination preparation, consultation, self-study = 8.5 h/ week*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	• *Basic software engineering concepts (software lifecycle, exception handling, threads/processes)* • *Basic operating systems knowledge (processes, concurrency, scheduling)* • *Basic distributed systems or networking fundamentals (optional but beneficial)* • *Basic probability/statistics and modelling concepts. This aligns with prerequisites seen in related courses (e.g., fault-tolerance courses that assume system architecture knowledge)*
Module objectives/intended learning outcomes	• *Explain key concepts of faults, errors, and failures in software systems.* • *Describe major software fault-tolerance techniques such as redundancy, recovery blocks, and checkpointing.* • *Apply software fault-tolerance strategies in system design and development.* • *Implement error detection and recovery mechanisms in software applications.* • *Analyze the dependability and reliability of software systems using modelling and evaluation methods.* • *Differentiate between hardware and software fault models and identify their implications in design.* • *Design and assess architectures for fault-tolerant and resilient software systems.* • *Evaluate trade-offs between reliability, performance, cost, and complexity in fault-tolerant systems.* • *Communicate reliability analysis results and design decisions effectively.*
Content	• *Introduction to software fault tolerance, dependability concepts, and system reliability*

	• *Software fault and error models: transient, permanent, and intermittent faults* • *Redundancy strategies: single-version and multi-version programming, recovery blocks* • *Exception handling, error detection, assertions, and monitoring* • *Checkpointing and rollback recovery in single and distributed systems* • *Software rejuvenation, fault injection, and self-healing mechanisms* • *Fault tolerance in concurrent and multi-threaded systems* • *Distributed software fault tolerance: replication, consensus, Byzantine faults, and fail-over* • *Dependability modelling and performance trade-offs in software systems* • *Fault tolerance in real-time and embedded systems* • *Fault tolerance in cloud and microservices environments: resilience patterns and service recovery* • *Case studies, project presentations, and course review*
Examination forms	***Exam*** ***Weight*** ***Date*** *Final* *60%* *TBA (to be announced)* *Laboratory* *20%* *every week* *Assignment* *20%* *TBA (to be announced)*
Study and examination requirements	*Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (60%)+Before Exam score will remain the same (40%)*
Reading list	• *I. Koren & C. M. Krishna, Fault-Tolerant Systems. 2nd Edition* • *P. Jalote, Fault Tolerance in Distributed Systems.* • *M. L. Shooman, Reliability of Computer Systems and Networks: Fault Tolerance, Analysis, and Design* • *Additional papers: on N-version programming, checkpointing, software rejuvenation, etc.*

Module designation	***IS 415 - Software Foundations for Cybersecurity***
Semester(s) in which the module is taught	*Year 4, fall semester*
Person responsible for the module	*Lecturer Orkhan Huseynli* *BHOS Bibiheybat Campus ROOM 420* *orkhan.huseynli@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Elective*
Teaching methods	*Lectures, presentation*
Workload (incl. contact hours, self-study hours)	*Total workload: 150 h = 102h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24h (2 h /week)* *Laboratory: 24h (2 h / week)s* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 8.5 h/ week*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	• *Basic programming skills (e.g., in at least one high-level language such as Python, Java or C)* • *Basic data structures & algorithms (arrays, lists, trees, graphs, algorithmic complexity)* • *Fundamentals of computer systems / operating systems (processes, memory, I/O)* • *Basic understanding of networks and web technologies (IP, HTTP, clients/servers)* • *Basic mathematics: logic, discrete mathematics, and probability/statistics at introductory level*
Module objectives/intended learning outcomes	• *Analyse how software architecture (modules, APIs, microservices), OS interactions, and networked contexts shape attack surfaces and trust boundaries, and diagram them for a given system.* • *Identify and reproduce common software & web vulnerabilities (e.g., buffer overflow, injection, XSS/CSRF, insecure deserialization) by creating minimal PoCs/tests that trigger each issue.* • *Apply secure-coding principles (input validation, output encoding, least privilege, safe error handling) to implement modules that pass all provided unit tests and static-analysis checks.* • *Use software analysis tools (static/dynamic analysis, fuzzing, code review) to detect, triage, and prioritize findings with a severity rationale and remediation notes.* • *Design secure software components and interfaces with appropriate security controls, logging/auditing, and exception-handling, and justify trade-offs among security, performance, and maintainability.* • *Evaluate security in networked/distributed environments (service communication, API security, client-server trust models) and implement at least one secure communication pattern in a lab task.* • *Integrate secure-development lifecycle practices (DevSecOps, CI/CD, patch management, container security) by configuring a pipeline*

<table>
<tr><td></td><td>step that enforces one security check (e.g., SAST/DAST/dependency scan).
• Implement software resilience and incident-response mechanisms (error logging, recovery, rollback) and validate them with test cases that simulate faults/adversarial inputs.
• Communicate clearly software security issues to stakeholders (developers, testers, managers) and propose remediation.</td></tr>
<tr><td>Content</td><td>• Introduction to software and cybersecurity: software lifecycle, threats, and vulnerabilities
• Software architecture fundamentals: modules, APIs, microservices, attack surfaces, and trust boundaries
• Secure coding principles: input validation, output encoding, least privilege, and safe error handling
• Common software vulnerabilities: buffer overflows, injection attacks, and memory safety issues
• Web and application vulnerabilities: SQL injection, XSS, CSRF, and insecure deserialization
• Software analysis and testing techniques: static and dynamic analysis, fuzzing, and code review
• Secure software design and architecture: defence-in-depth, auditing, and exception-handling strategies
• Software in networked and distributed environments: service communication, API security, and client-server trust models
• Secure development lifecycle: DevSecOps, CI/CD security, patch management, and container security
• Software resilience and incident response: error logging, recovery, and rollback mechanisms
• Emerging topics: software supply chain security, IoT, mobile, and cloud-native software vulnerabilities
• Case studies, student presentations, and integration of software and cybersecurity concepts</td></tr>
<tr><td>Examination forms</td><td><table><tr><th>Exam</th><th>Weight</th><th>Date</th></tr><tr><td>Final</td><td>50%</td><td>TBA (to be announced)</td></tr><tr><td>Quiz</td><td>20%</td><td>every week</td></tr><tr><td>Presentation</td><td>20%</td><td>TBA (to be announced)</td></tr><tr><td>Activity</td><td>10%</td><td></td></tr></table></td></tr>
<tr><td>Study and examination requirements</td><td>Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (50%)+Before Exam score will remain the same (50%)</td></tr>
<tr><td>Reading list</td><td>• McGraw, G. Software Security: Building Security In. Addison-Wesley, 2006.
• Howard, M., LeBlanc, D. Writing Secure Code. 2nd Edition. Microsoft Press, 2009.
• Halfond, W., Orso, A., & Manolescu, D. (eds) Proceedings of Software Security and Reliability.
• OWASP Top 10 (community resource) for web/application vulnerabilities.
You can also draw on course materials from institutions offering “Foundations of Cybersecurity” or “Foundations of Software Security” based on research.</td></tr>
</table>

Module designation	***IS 417 - System Programming***
Semester(s) in which the module is taught	*Year 4, fall semester*
Person responsible for the module	*Lecturer Kamran Hasanov* *BHOS Bibiheybat Campus ROOM 420* *kamran.hasanov@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Elective*
Teaching methods	*Lectures, presentation*
Workload (incl. contact hours, self-study hours)	*Total workload: 150 h = 102h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24h (2 h /week)* *Laboratory: 24h (2 h / week)s* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 8.5 h/ week*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	• *Proficiency in C programming (including pointers, structs, memory management)* • *Basic understanding of computer architecture and operating systems* • *Familiarity with Linux command-line tools and scripting*
Module objectives/intended learning outcomes	• *Understand and utilize system calls for process and memory management.* • *Develop and manage processes using fork(), exec(), and wait().* • *Implement inter-process communication mechanisms like pipes and message queues.* • *Handle file I/O operations, including buffered and unbuffered techniques.* • *Manage memory dynamically and understand memory allocation strategies.* • *Analyze and manipulate system-level data structures.* • *Implement basic synchronization primitives for concurrent programming.* • *Develop and debug system-level applications using tools like gdb.*
Content	• *Introduction to System Programming: Overview of system programming, role of system calls, and the Linux programming environment.* • *Processes and Process Control: Creating and managing processes, process states, and process control blocks.* • *System Calls and the Kernel Interface: Understanding system calls, their role in system programming, and interaction with the kernel.* • *Memory Management: Dynamic memory allocation, memory leaks, and garbage collection techniques.* • *File I/O Operations: Handling file descriptors, file permissions, and file system interfaces.*

	• *Inter-Process Communication (IPC): Implementing pipes, message queues, and shared memory.* • *Concurrency and Synchronization: Threads, mutexes, semaphores, and avoiding race conditions.* • *Signal Handling: Understanding and handling Unix signals for process control.* • *Networking Basics: Sockets, client-server model, and basic network programming.* • *Security Considerations: Buffer overflows, input validation, and secure coding practices.* • *Debugging and Profiling: Using gdb, valgrind, and performance profiling tools.* • *Project Presentations and Review: Student presentations of final projects and course review.*
Examination forms	***Exam*** ***Weight*** ***Date*** *Final* *60%* *TBA (to be announced)* *Quiz* *20%* *every week* *Presentation* *20%* *TBA (to be announced)*
Study and examination requirements	*Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (40%)+Before Exam score will remain the same (60%)*
Reading list	• *"The C Programming Language" by Brian W. Kernighan and Dennis M. Ritchie* • *"Advanced Programming in the UNIX Environment" by W. Richard Stevens* • *"Computer Systems: A Programmer's Perspective" by Randal E. Bryant and David R. O'Hallaron*

Module designation	***IS 419 - System Administration***
Semester(s) in which the module is taught	*Year 4, fall semester*
Person responsible for the module	*Lecturer Kamran Hasanov* *BHOS Bibiheybat Campus ROOM 420* *kamran.hasanov@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Elective*
Teaching methods	*Lectures, presentation*
Workload (incl. contact hours, self-study hours)	*Total workload: 150 h = 102h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24h (2 h /week)* *Laboratory: 24h (2 h / week)s* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 8.5 h/ week*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	• ***Operating System Fundamentals*** *– understanding processes, memory, file systems, and system architecture.* • ***Networking Basics*** *– IP addressing, TCP/IP, DNS, DHCP, and client-server concepts.* • ***Command-Line Proficiency*** *– using Windows Command Prompt, PowerShell, or Linux Bash.* • ***Software Installation & Configuration*** *– ability to install, configure, and manage applications and system services.*
Module objectives/intended learning outcomes	• *Understand the architecture and core components of Windows Server 2025* • *Install, configure, and manage Windows Server using Server Manager and PowerShell* • *Configure and manage Active Directory Domain Services (AD DS)* • *Create and manage users, groups, and organizational units (OUs)* • *Install and configure DNS and DHCP server roles* • *Apply Group Policy Objects (GPO) for centralized system and user management* • *Configure file shares, NTFS permissions, and storage services* • *Deploy operating systems using Windows Deployment Services (WDS)* • *Manage updates using Windows Server Update Services (WSUS)*
Content	• *Windows Server 2025 Overview* • *Installation and Configuration of Windows Server* • *Server Roles and Services (AD DS, DHCP, DNS, File Services)* • *Introduction to Active Directory Domain Services (AD DS)* • *User, Group, and DNS Management* • *Group Policy Objects (GPO)* • *Quizzes / Mid-course Assessment* • *DHCP Service Installation and Configuration*

<table>
<tr><td></td><td>

- *File Services and Storage Management (NTFS, DFS, Shadow Copies)*
- *Windows Deployment Services (WDS) and Image Management*
- *Windows Server Update Services (WSUS) Management*
- *Backup and Disaster Recovery*

</td></tr>
<tr><td>Examination forms</td><td>

Exam	***Weight***	***Date***
Final	*40%*	*TBA (to be announced)*
Quiz	*20%*	*every week*
Laboratory	*20%*	*every 2 weeks*
Presentation	*20%*	*TBA (to be announced)*

</td></tr>
<tr><td>Study and examination requirements</td><td>Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (40%)+Before Exam score will remain the same (60%)</td></tr>
<tr><td>Reading list</td><td>

- *Microsoft Press. Mastering Windows Server 2022 (latest edition as reference for 2025 updates)*
- *Mark Minasi. Mastering Windows Server 2022 Administration*
- *Orin Thomas. Windows Server 2022 Inside Out*
- *Microsoft. Windows Server 2025 Documentation – official documentation online*

</td></tr>
</table>

Module designation	***IS 410 - Applied Cryptography***
Semester(s) in which the module is taught	*Year 4, spring semester*
Person responsible for the module	*Lecturer Nihad Alili* *BHOS Bibiheybat Campus ROOM 420* *nihad.elili@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Elective*
Teaching methods	*Lectures, laboratory, presentation, quizzes*
Workload (incl. contact hours, self-study hours)	*Total workload: 150 h = 102h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24h (2 h /week)* *Laboratory: 24h (2 h / week)s* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 8.5 h/ week*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	• *Mathematical Maturity: Ability to read and write mathematical definitions, statements, and proofs.* • *Discrete Mathematics: Familiarity with topics such as sets, functions, relations, and combinatorics.* • *Algorithms and Complexity: Understanding of algorithm design, analysis, and computational complexity.* • *Probability Theory: Basic knowledge of probability, random variables, and distributions.* • *Programming Skills: Proficiency in at least one programming language (e.g., Python, C++).* • *Operating Systems: Basic understanding of operating system concepts and command-line interfaces.*
Module objectives/intended learning outcomes	• *Explain the theoretical foundations of modern cryptography and classical ciphers.* • *Analyze the security of cryptographic algorithms and protocols.* • *Implement encryption, decryption, and hashing using contemporary cryptographic libraries.* • *Apply digital signatures and message authentication codes to secure communications.* • *Understand key exchange protocols and secure communication mechanisms like TLS/SSL.* • *Evaluate cryptographic systems for vulnerabilities and resistance to attacks.* • *Describe emerging cryptographic techniques, including post-quantum cryptography.* • *Apply cryptography in real-world scenarios such as blockchain, secure messaging, and data privacy.*
Content	• *Introduction to Cryptography: history, goals, applications*

<table>
<tr><td></td><td>

- *Classical Cryptosystems: Caesar, Vigenère, substitution, and transposition ciphers*
- *Symmetric Key Cryptography: block ciphers (DES, AES) and modes of operation*
- *Public Key Cryptography: RSA, Diffie-Hellman key exchange, and key management*
- *Hash Functions: MD5, SHA families, properties, and applications*
- *Digital Signatures: RSA signatures, DSA, ECDSA, and authentication*
- *Message Authentication Codes (MACs) and HMAC/CMAC*
- *Cryptographic Protocols and Secure Communications: TLS/SSL, IPSec, Kerberos*
- *Cryptanalysis: brute force, birthday paradox, side-channel attacks*
- *Post-Quantum Cryptography: lattice-based, NTRU, and LWE schemes*
- *Blockchain and Cryptocurrencies: Bitcoin, Ethereum, consensus mechanisms*
- *Privacy-Preserving Cryptography & Real-World Applications: homomorphic encryption, secure multi-party computation, final project presentations*

</td></tr>
<tr><td>Examination forms</td><td>

Exam	***Weight***	***Date***
Final	*60%*	*TBA (to be announced)*
Quiz	*20%*	*every week*
Presentation	*20%*	*TBA (to be announced)*

</td></tr>
<tr><td>Study and examination requirements</td><td>*Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (60%)+Before Exam score will remain the same (40%)*</td></tr>
<tr><td>Reading list</td><td>

- *"Introduction to Modern Cryptography" (3rd Edition) by Jonathan Katz and Yehuda Lindell.*
- *"Applied Cryptography: Protocols, Algorithms, and Source Code in C" by Bruce Schneier.*
- *"Understanding Cryptography: A Textbook for Students and Practitioners" by Christof Paar and Jan Pelzl.*

</td></tr>
</table>

Module designation	***IS 412 - Attacker Tools and Techniques***
Semester(s) in which the module is taught	*Year 4, spring semester*
Person responsible for the module	*Lecturer Nihad Alili* *BHOS Bibiheybat Campus ROOM 420* *nihad.elili@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Elective*
Teaching methods	*Lectures, laboratory, presentation*
Workload (incl. contact hours, self-study hours)	*Total workload: 150 h = 102h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24h (2 h /week)* *Laboratory: 24h (2 h / week)s* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 8.5 h/ week*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	• ***Operating Systems & Shells*** *— comfortable with Windows and Linux basics (file systems, processes, services).* • ***Networking Fundamentals*** *— TCP/IP, ports, DNS, common protocols (HTTP, SMTP), and basic packet concepts.* • ***Programming / Scripting*** *— ability to read and write simple scripts (Python, Bash, PowerShell).* • ***Foundations of Cybersecurity*** *— familiarity with cryptography basics, authentication concepts, and common vulnerabilities.*
Module objectives/intended learning outcomes	*After this course students will be able to:* • *Explain the attacker kill-chain and how common offensive techniques map to each phase.* • *Identify and categorise classes of attacker tools (reconnaissance, scanning, exploitation frameworks, post-exploitation, C2, malware, evasion).* • *Analyse attacker trade-offs (stealth vs speed, persistence vs footprint) and likely indicators of compromise.* • *Evaluate telemetry (logs, network flows, endpoint signals) to detect and triage offensive activity.* • *Describe common attack patterns and the defenses/controls that mitigate them (hardening, segmentation, detection rules).* • *Demonstrate safe, legal lab practices for testing in an isolated environment (sandboxing, virtualization, network isolation).* • *Use attacker-knowledge to improve secure design, incident response playbooks, and detection signatures (conceptually — not by producing offensive exploits).* • *Discuss ethical, legal and policy issues related to vulnerability research, disclosure and penetration testing.*

Content	• *Attacker Mindset & Legal/Ethical Frameworks* • *Reconnaissance & OSINT* • *Network Scanning & Service Discovery* • *Vulnerability Classes & Exploit Anatomy* • *Exploitation Frameworks (conceptual)* • *Web Attacks & Application-layer Techniques* • *Malware Fundamentals & Analysis Principles* • *Command & Control (C2) & Lateral Movement* • *Evasion, Anti-Forensics & Persistence* • *Post-Exploitation & Data Exfiltration* • *Defensive Use of Attacker Knowledge*
Examination forms	***Exam*** ***Weight*** ***Date*** *Final* *60%* *TBA (to be announced)* *Laboratory* *20%* *every week* *Presentation* *20%* *TBA (to be announced)*
Study and examination requirements	*Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (40%)+Before Exam score will remain the same (60%)*
Reading list	1. ***Jon Erickson.*** *Hacking: The Art of Exploitation (2nd Edition). No Starch Press, 2008.* 2. ***Georgia Weidman.*** *Penetration Testing: A Hands-On Introduction to Hacking.* 3. ***Peter Kim.*** *The Hacker Playbook 3: Practical Guide To Penetration Testing.*

Module designation	***IS 414 - Fundamentals of Disaster Recovery***
Semester(s) in which the module is taught	*Year 4, spring semester*
Person responsible for the module	*Lecturer Nihad Alili* *BHOS Bibiheybat Campus ROOM 420* *elili.nihad@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Elective*
Teaching methods	*Lectures, laboratory, quizzes, class activities*
Workload (incl. contact hours, self-study hours)	*Total workload: 150 h = 102h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24h (2 h /week)* *Laboratory: 24h (2 h / week)s* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 8.5 h/ week*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	• *Basic understanding of Information Security principles* • *Knowledge of IT systems and networks* • *Fundamentals of Operating Systems and storage systems* • *Basic familiarity with risk management concepts*
Module objectives/intended learning outcomes	*By the end of the course, students will be able to:* • *Explain the principles and importance of disaster recovery and business continuity.* • *Identify and assess potential IT and operational risks.* • *Design disaster recovery plans and procedures for IT systems.* • *Evaluate recovery strategies, backup solutions, and failover techniques.* • *Implement testing and maintenance strategies for disaster recovery plans.* • *Apply legal, compliance, and organizational requirements in DR planning.* • *Analyze real-world disaster recovery scenarios and lessons learned.*
Content	• *Introduction to Disaster Recovery (DR) and Business Continuity (BC)* • *Risk assessment and business impact analysis* • *Disaster recovery policies and planning frameworks* • *Backup strategies and technologies (full, incremental, differential)* • *Recovery strategies for servers, databases, and networks* • *High availability and failover mechanisms* • *Cloud-based disaster recovery solutions* • *Data replication and synchronization techniques*

<table>
<tr><td></td><td>

- *Testing and validation of DR plans*
- *Incident response and communication planning*
- *Compliance, legal, and regulatory considerations*

</td></tr>
<tr><td>Examination forms</td><td>

Exam	***Weight***	***Date***
Final	*60%*	*TBA (to be announced)*
Laboratory	*20%*	*every week*
Quiz	*20%*	*TBA (to be announced)*

</td></tr>
<tr><td>Study and examination requirements</td><td>Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (60%)+Before Exam score will remain the same (40%)</td></tr>
<tr><td>Reading list</td><td>

- *Wallace, M., Webber, L., The Disaster Recovery Handbook, 3rd Edition*
- *Rittinghouse, J., Ransome, J., Disaster Recovery and Business Continuity, 2nd Edition*
- *Snedaker, S., Business Continuity and Disaster Recovery Planning for IT Professionals, 4th Edition*
- *NIST Special Publication 800-34: Contingency Planning Guide for Federal Information Systems*

</td></tr>
</table>

Module designation	***IS 416 - Microservices***
Semester(s) in which the module is taught	*Year 4, spring semester*
Person responsible for the module	*Lecturer Khayyam Masiyev* *BHOS Bibiheybat Campus ROOM 420* *khayyam.masiyev@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Elective*
Teaching methods	*Lectures, presentation*
Workload (incl. contact hours, self-study hours)	*Total workload: 150 h = 102h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24h (2 h /week)* *Laboratory: 24h (2 h / week)s* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 8.5 h/ week*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	• *Programming experience in Java, Python, or Node.js* • *Understanding of object-oriented programming (OOP)* • *Basic knowledge of web development (HTTP, REST APIs, JSON)* • *Fundamentals of databases and networking*
Module objectives/intended learning outcomes	*By the end of the course, students will be able to:* • *Explain the microservices architecture and its advantages over monolithic systems.* • *Design and implement scalable, loosely coupled microservices.* • *Develop RESTful APIs for communication between services.* • *Apply service discovery, load balancing, and API gateway patterns.* • *Implement security, logging, and monitoring in microservices.* • *Utilize containerization and orchestration tools (Docker, Kubernetes).* • *Evaluate trade-offs in scalability, maintainability, and performance.* • *Troubleshoot and test microservices in development and production environments.*
Content	• *Introduction to Microservices Architecture and Principles* • *Monolithic vs Microservices: Advantages and Challenges* • *Designing Microservices: Boundaries, Domain-Driven Design (DDD)* • *RESTful APIs and Inter-Service Communication* • *Service Discovery and Load Balancing* • *API Gateway and Messaging Patterns* • *Database Strategies: Polyglot Persistence and Data Consistency* • *Security in Microservices: Authentication, Authorization, and Tokens* • *Logging, Monitoring, and Observability* • *Containerization with Docker for Microservices* • *Orchestration with Kubernetes and CI/CD Pipelines*

Examination forms	***Exam***	***Weight***	***Date***
	Final	*60%*	*TBA (to be announced)*
	Quiz	*20%*	*every week*
	Presentation	*20%*	*TBA (to be announced)*
Study and examination requirements	*Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (40%)+Before Exam score will remain the same (60%)*		
Reading list	• *Newman, S., Building Microservices, 2nd Edition, O'Reilly, 2021* • *Richardson, C., Microservices Patterns: With examples in Java, Manning, 2018* • *Hohpe, G., Enterprise Integration Patterns, Addison-Wesley, 2003* • *Fowler, M., Microservices: A Definition of This New Architectural Term, martinfowler.com* • *Official Docker and Kubernetes Documentation*		

Module designation	***IS 418 - SCADA security***
Semester(s) in which the module is taught	*Year 4, spring semester*
Person responsible for the module	*Lecturer Elshan Rahimov* *BHOS Bibiheybat Campus ROOM 420* *elshan.rahimov@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Elective*
Teaching methods	*Lectures, laboratory, presentation*
Workload (incl. contact hours, self-study hours)	*Total workload: 150 h = 102h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24h (2 h /week)* *Laboratory: 24h (2 h / week)s* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 8.5 h/ week*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	• *Fundamentals of industrial control systems (ICS) and SCADA)* • *Basic networking concepts (TCP/IP, Modbus/TCP, Ethernet)* • *Understanding of operating systems (Windows/Linux)* • *Knowledge of cybersecurity principles and threat modeling*
Module objectives/intended learning outcomes	*By the end of the course, students will be able to:* • *Explain SCADA system architecture, components, and communication protocols.* • *Identify security risks and vulnerabilities in SCADA/ICS environments.* • *Analyze attack vectors specific to industrial control systems.* • *Apply best practices for securing SCADA networks and devices.* • *Implement monitoring, logging, and intrusion detection tailored for ICS.* • *Evaluate regulatory and compliance requirements for critical infrastructure.* • *Conduct risk assessment and develop SCADA-specific incident response strategies.* • *Understand emerging trends and threats in industrial cybersecurity.*
Content	• *Introduction to SCADA and Industrial Control Systems (ICS)* • *SCADA Architecture: RTUs, PLCs, HMI, and network layers* • *SCADA Communication Protocols: Modbus, DNP3, OPC, IEC 60870-5-104* • *Common SCADA Vulnerabilities and Threat Landscape* • *Cyberattack Techniques in SCADA Environments* • *Network Segmentation, Firewalls, and Security Zones* • *Authentication, Access Control, and Secure Remote Access*

<table>
<tr><td></td><td>

- *Intrusion Detection and Monitoring for ICS*
- *Malware and Threat Intelligence in Industrial Systems*
- *Backup, Recovery, and Incident Response in SCADA*
- *Regulatory Compliance and Industry Standards (NERC-CIP, IEC 62443)*

</td></tr>
<tr><td>Examination forms</td><td>

Exam	***Weight***	***Date***
Final	*60%*	*TBA (to be announced)*
Laboratory	*20%*	*every week*
Presentation	*20%*	*TBA (to be announced)*

</td></tr>
<tr><td>Study and examination requirements</td><td>Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (60%)+Before Exam score will remain the same (40%)</td></tr>
<tr><td>Reading list</td><td>

- *Stouffer, K., Falco, J., Scarfone, K., Guide to Industrial Control Systems (ICS) Security, NIST SP 800-82*
- *Nicholson, A., Webber, S., Dyer, S., Patel, T., Janicke, H., SCADA Security in Critical Infrastructure, Elsevier, 2012*
- *Krutz, R. L., Securing SCADA Systems, Wiley, 2011*
- *IEC 62443 Standards for Industrial Automation Security*
- *Modbus/TCP, DNP3, and OPC official protocol documentation*

</td></tr>
</table>

Module designation	***IS 420 - Attacks on Cryptosystems***
Semester(s) in which the module is taught	*Year 4, spring semester*
Person responsible for the module	*Lecturer Nihad Alili* *BHOS Bibiheybat Campus ROOM 420* *nihad.elili@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Elective*
Teaching methods	*Lectures, laboratory, presentation*
Workload (incl. contact hours, self-study hours)	*Total workload: 150 h = 102h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24h (2 h /week)* *Laboratory: 24h (2 h / week)s* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 8.5 h/ week*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	• *Modern cryptography fundamentals (symmetric/asymmetric crypto, hash functions, MACs)* • *Probability & discrete mathematics (basic proofs, number theory exposure helpful)* • *Algorithms & complexity (big-O, basic complexity classes)* • *Programming ability (Python or similar) and familiarity with crypto libraries*
Module objectives/intended learning outcomes	*By the end of the course students will be able to:* • *Classify major classes of cryptanalytic attacks (ciphertext-only, known-plaintext, chosen-plaintext/-ciphertext, side-channel, fault, protocol-level).* • *Explain theoretical foundations that enable attacks (e.g., algebraic structure, statistical weaknesses, implementation leakage).* • *Assess the practical feasibility and cost of attacks against real-world schemes.* • *Interpret historical cryptographic failures and extract lessons for secure design.* • *Analyse protocol weaknesses and demonstrate how design flaws lead to exploitation (at a conceptual level).* • *Evaluate countermeasures and mitigations for different attack classes.* • *Apply safe, legal laboratory methods to reproduce non-destructive experiments (e.g., simulations, microbenchmarks) for research/defensive purposes.* • *Communicate findings clearly, including ethical and disclosure implications.*

<table>
<tr><td>Content</td><td>

- *Introduction & Ethics in Cryptanalysis*
- *Classical Cryptanalysis: frequency & statistical attacks*
- *Block Cipher Attacks: differential & linear cryptanalysis*
- *Stream Cipher & PRNG Weaknesses*
- *Hash Function Attacks: collision, preimage, length-extension*
- *Public-Key Attacks: factoring, discrete log, padding oracle*
- *Side-Channel Attacks: timing, power, EM leakage*
- *Fault Attacks & Implementation Vulnerabilities*
- *Protocol-Level Attacks: MITM, downgrade, replay*
- *Automated & Algebraic Attacks: lattice, algebraic cryptanalysis*
- *Post-Quantum Considerations & Threats*

</td></tr>
<tr><td>Examination forms</td><td>

Exam	***Weight***	***Date***
Final	*60%*	*TBA (to be announced)*
Laboratory	*20%*	*every week*
Presentation	*20%*	*TBA (to be announced)*

</td></tr>
<tr><td>Study and examination requirements</td><td>Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure, the student can also be given a chance to retake the exam. Resit Exam score (60%) + Before Exam score will remain the same (40%)</td></tr>
<tr><td>Reading list</td><td>

- *Katz, J. & Lindell, Y., Introduction to Modern Cryptography*
- *Menezes, A., van Oorschot, P., Vanstone, S., Handbook of Applied Cryptography*
- *Paar, C. & Pelzl, J., Understanding Cryptography*
- *Boneh, D. & Shoup, V., A Graduate Course in Applied Cryptography*

</td></tr>
</table>

Module designation	***IS 422 - DevOps***
Semester(s) in which the module is taught	*Year 4, spring semester*
Person responsible for the module	*Lecturer Elshan Farzaliyev* *BHOS Bibiheybat Campus ROOM 420* *elshan.farzaliyev@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Elective*
Teaching methods	*Lectures, presentation*
Workload (incl. contact hours, self-study hours)	*Total workload: 150 h = 102h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24h (2 h /week)* *Laboratory: 24h (2 h / week)s* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 8.5 h/ week*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	• *Basic programming or scripting (Python, Bash, etc.)* • *Operating systems and command-line familiarity (Windows/Linux)* • *Version control and software development concepts (Git, SDLC)* • *Basic networking and web protocols (TCP/IP, HTTP/HTTPS)*
Module objectives/intended learning outcomes	• *Explain DevOps principles and the roles of CI/CD, mapping them to different team and project contexts.* • *Design and implement a minimal CI pipeline (build + test + artifact) and demonstrate that it runs automatically on each push.* • *Containerize a service with a well-structured Dockerfile, publish the image to a registry, and justify base-image and security choices.* • *Deploy the service on Kubernetes (Deployment, Service, Config/Secret) and perform a safe rollback scenario* • *Apply Infrastructure-as-Code (e.g., Ansible/Terraform) to provision an environment and verify idempotency with repeatable runs.* • *Instrument and monitor an application (metrics, logs, traces), define at least two SLOs, and triage an incident with a documented root-cause analysis.* • *Evaluate and justify trade-offs among performance, reliability, cost, and security when selecting deployment and release strategies (e.g., blue-green, canary).*
Content	• *Introduction to DevOps: principles, culture, toolchain* • *Version Control & Git: basics, branching, collaboration* • *Continuous Integration (CI): pipelines, automated testing* • *Docker: containerization concepts and usage* • *Continuous Delivery & Deployment (CD) concepts*

<table>
<tr><td></td><td>

Kubernetes: architecture, pods, services, deployments
Deployment Strategies: blue-green, canary, rollback
Infrastructure as Code (IaC) with Ansible
Monitoring & Logging: Prometheus, Grafana, alerts
Docker Hands-On: Dockerfiles, image creation
Kubernetes Hands-On: deploying and managing services

</td></tr>
<tr><td>Examination forms</td><td>
<table>
<tr><th>Exam</th><th>Weight</th><th>Date</th></tr>
<tr><td>Final</td><td>50%</td><td>TBA (to be announced)</td></tr>
<tr><td>Laboratory</td><td>30%</td><td>every week</td></tr>
<tr><td>Presentation</td><td>20%</td><td>TBA (to be announced)</td></tr>
</table>
</td></tr>
<tr><td>Study and examination requirements</td><td>Student is normally expected to achieve a total mark (pre-exam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure, the student can also be given a chance to retake the exam. Resit Exam score (40%) +Before Exam score will remain the same (60%)</td></tr>
<tr><td>Reading list</td><td>

Scott Chacon & Ben Straub, Pro Git
Gene Kim, Jez Humble, Patrick Debois, John Willis – The DevOps Handbook: How to Create World-Class Agility, Reliability, and Security in Technology Organizations
Nicole Forsgren, Gene Kim, Jez Humble – Accelerate: The Science of Lean Software and DevOps
Kief Morris – Infrastructure as Code: Managing Servers in the Cloud

</td></tr>
</table>

Module designation	***IS 509 - Design and Analysis of Secure Protocols***
Semester(s) in which the module is taught	*Year 5, fall semester*
Person responsible for the module	*Lecturer Mehran Hematyar* *BHOS Bibiheybat Campus ROOM 420* *mehran.hematyar@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Elective*
Teaching methods	*Lectures, laboratory work, presentation, quizzes*
Workload (incl. contact hours, self-study hours)	*Total workload: 150 h = 102h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24h (2 h /week)* *Laboratory: 24h (2 h / week)s* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 8.5 h/ week*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	• *Fundamentals of cryptography (symmetric/asymmetric encryption, hash functions, digital signatures)* • *Basic networking concepts (TCP/IP, sockets, HTTP/HTTPS)* • *Programming experience (Python, Java, or C/C++)* • *Foundations of information security (authentication, confidentiality, integrity)*
Module objectives/intended learning outcomes	*By the end of the course, students will be able to:* • *Explain the principles of secure protocol design and common security goals.* • *Analyze protocols for potential vulnerabilities and attacks.* • *Design protocols that provide confidentiality, integrity, authentication, and non-repudiation.* • *Evaluate real-world protocols (TLS, IPSec, Kerberos, OAuth) for security strengths and weaknesses.* • *Apply formal methods and reasoning to verify protocol correctness.* • *Understand key exchange, authentication mechanisms, and session management.* • *Demonstrate secure implementation practices and mitigation strategies.*
Content	• *Introduction to Secure Protocols and Security Goals* • *Cryptographic Primitives in Protocol Design* • *Authentication Protocols and Password-based Schemes* • *Key Exchange Protocols (Diffie-Hellman, Public-Key)* • *Digital Signatures and Message Authentication Codes (MACs)* • *Session Management and Secure Channel Establishment*

<table>
<tr><td></td><td>

- *TLS / SSL Protocol Design and Analysis*
- *IPSec and VPN Protocols*
- *Kerberos and Ticket-based Authentication*
- *OAuth, OpenID Connect, and Modern Web Protocol Security*
- *Formal Methods for Protocol Verification*

</td></tr>
<tr><td>Examination forms</td><td>

Exam	***Weight***	***Date***
Final	*40%*	*TBA (to be announced)*
Quiz	*20%*	*TBA (to be announced)*
Laboratory	*20%*	*every week*
Presentation	*20%*	*TBA (to be announced)*

</td></tr>
<tr><td>Study and examination requirements</td><td>Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (40%)+Before Exam score will remain the same (60%)</td></tr>
<tr><td>Reading list</td><td>

- *William Stallings, Cryptography and Network Security, 8th Edition*
- *Bruce Schneier, Applied Cryptography, 2nd Edition*
- *Koblitz & Menezes, The Handbook of Applied Cryptography*
- *Ross Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems*

</td></tr>
</table>

Module designation	***IS 511 - Open-Source Intelligence***
Semester(s) in which the module is taught	*Year 5, fall semester*
Person responsible for the module	*Lecturer Elvin Abaszade* *BHOS Bibiheybat Campus ROOM 420* *Elvin.abaszade@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Elective*
Teaching methods	*Lectures, presentation*
Workload (incl. contact hours, self-study hours)	*Total workload: 150 h = 102h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24h (2 h /week)* *Laboratory: 24h (2 h / week)s* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 8.5 h/ week*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	• *Basic understanding of information security and cybersecurity principles* • *Familiarity with internet, social media platforms, and search engines* • *Basic networking and web technologies (HTTP, DNS, APIs)* • *Introductory research and analytical skills*
Module objectives/intended learning outcomes	*By the end of the course, students will be able to:* • *Explain the principles, methodologies, and ethical/legal considerations of OSINT.* • *Collect and analyze publicly available information from multiple sources.* • *Evaluate the reliability and credibility of OSINT sources.* • *Utilize OSINT tools and techniques for structured data collection.* • *Apply OSINT to support cybersecurity, investigations, and threat intelligence.* • *Understand data privacy, legal constraints, and responsible reporting practices.* • *Prepare professional OSINT reports and communicate findings effectively*
Content	• *Introduction to OSINT: concepts, principles, and ethical considerations* • *Internet and search engine intelligence techniques* • *Social media intelligence (SOCMINT) and analysis* • *Geospatial intelligence (GEOINT) and mapping tools* • *Dark web and specialized OSINT sources*

	• *Public records and corporate data collection* • *Email, domain, and IP intelligence* • *Automated data collection and scraping techniques* • *OSINT frameworks, platforms, and open-source tools* • *Threat intelligence integration and analysis* • *Legal, privacy, and ethical aspects of OSINT*
Examination forms	***Exam*** ***Weight*** ***Date*** *Final* *60%* *TBA (to be announced)* *Quiz* *20%* *every week* *Presentation* *20%* *TBA (to be announced)*
Study and examination requirements	*Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (40%)+Before Exam score will remain the same (60%)*
Reading list	• *Michael Bazzell, Open Source Intelligence Techniques (latest edition)* • *Stewart K., OSINT for Cybersecurity* • *Christopher J. Hadnagy, Social Engineering: The Science of Human Hacking (for SOCMINT insights)*

Module designation	***IS 513 - Cryptocurrency***
Semester(s) in which the module is taught	*Year 5, fall semester*
Person responsible for the module	*Nihad Alili* *BHOS Bibiheybat Campus ROOM 420* *nihad.elili@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Elective*
Teaching methods	*Lectures, Presentations, Practical demonstrations, and Discussions*
Workload (incl. contact hours, self-study hours)	*Total workload: 150 h = 102h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24h (2 h /week)* *Laboratory: 24h (2 h / week)s* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 8.5 h/ week*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	*• Basic understanding of information security and blockchain fundamentals.* *• Familiarity with Internet and networking concepts.* *• Introductory programming or analytical skills are recommended.*
Module objectives/intended learning outcomes	*By the end of the course, students will be able to:* *1. Explain the history, evolution, and significance of cryptocurrencies.* *2. Demonstrate understanding of cryptographic mechanisms including hashing, public/private keys, and digital signatures.* *3. Compare consensus mechanisms (Proof-of-Work, Proof-of-Stake, etc.) and analyze their trade-offs.* *4. Conduct basic cryptocurrency transactions and utilize digital wallets.* *5. Deploy and test simple smart contracts on the Ethereum platform.* *6. Evaluate real-world security challenges, exchange hacks, and attack vectors.* *7. Analyze the economic and regulatory frameworks governing digital currencies.* *8. Prepare a professional group presentation or project on cryptocurrency applications.*

Content	• *Introduction to Cryptocurrencies – History of money, emergence of Bitcoin, motivation for cryptocurrencies.* • *Technical Foundations of Bitcoin – Blockchain structure, peer-to-peer networking, and the double-spending problem.* • *Cryptography and Security Principles – Hashing, asymmetric encryption, and digital signatures.* • *Consensus Mechanisms and Mining – Proof-of-Work, Proof-of-Stake, and mining attacks (51%)* • *Economics of Cryptocurrencies – Supply, demand, volatility, and valuation.* • *Digital Wallets and Transactions – Wallet types, UTXO model, and transaction lifecycle.* • *Blockchain Platforms (Ethereum) – Accounts, EVM, gas, and architectural comparison.* • *Smart Contracts – Solidity fundamentals and security considerations.* • *Decentralized Applications (DApps) and DeFi – Token standards, decentralized finance, and governance.* • *Cryptocurrency Security and Attacks – Common vulnerabilities, hacks, and mitigations.* • *Stablecoins, CBDCs, and Regulation – Legal frameworks, AML/KYC, and global responses.* • *Future Trends – NFTs, Web3, and future of digital finance.*
Examination forms	***Exam*** ***Weight*** ***Date*** *Final* *60%* *TBA (to be announced)* *Quiz* *20%* *every week* *Presentation* *20%* *TBA (to be announced)*
Study and examination requirements	*Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure, the student can also be given a chance to retake the exam. Resit Exam score (40%) +Before Exam score will remain the same (60%)*
Reading list	• *Antonopoulos, A. M. & Harding, D. A. (2023). Mastering Bitcoin: Programming the Open Blockchain (3rd Ed.), O'Reilly.* • *Antonopoulos, A. M. & Wood, G. (2018). Mastering Ethereum: Building Smart Contracts and DApps, O'Reilly.* • *Vigna, P., & Casey, M. J. (2015). The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order, St. Martin's Press.* • *Bashir, I. (2020). Mastering Blockchain (3rd Ed.), Packt Publishing.*

Module designation	***IS 515 - Reverse Engineering***
Semester(s) in which the module is taught	*Year 5, fall semester*
Person responsible for the module	*Lecturer Nihad Alili* *BHOS Bibiheybat Campus ROOM 420* *nihad.alili@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Elective*
Teaching methods	*Lectures, laboratory, presentation*
Workload (incl. contact hours, self-study hours)	*Total workload: 150 h = 102h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24h (2 h /week)* *Laboratory: 24h (2 h / week)s* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 8.5 h/ week*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	• *Programming experience in C/C++ or Python* • *Understanding of computer architecture and operating systems* • *Basic knowledge of assembly language and memory management* • *Fundamentals of cybersecurity and malware analysis*
Module objectives/intended learning outcomes	*By the end of the course, students will be able to:* • *Explain the principles and purposes of reverse engineering.* • *Analyze software binaries and understand program execution flow.* • *Disassemble and decompile applications to extract logic.* • *Identify vulnerabilities and potential security weaknesses in programs.* • *Understand obfuscation, packing, and anti-reverse engineering techniques.* • *Apply dynamic and static analysis tools effectively.* • *Conduct safe and ethical reverse engineering in controlled environments.* • *Prioritize and quantify the security impact of discovered findings using standard risk models (e.g., CVSS) and evidence-based reasoning.* • *Propose concrete mitigations and secure design changes that address the root causes revealed by reverse engineering.* • *Plan and execute reproducible reverse-engineering experiments; collect, preserve, and reference evidence (artifacts, traces, PoCs) with proper methodology.* • *Produce a structured technical RE report and deliver a clear oral presentation that explains methods, evidence, risks, and*

	recommended controls to specialist and non-specialist audiences.
Content	• *Introduction to Reverse Engineering: concepts, ethics, and legal considerations* • *Overview of software binaries and executable formats (PE, ELF, Mach-O)* • *Assembly language fundamentals for reverse engineering* • *Static analysis: disassembly, decompilers, and code inspection* • *Dynamic analysis: debuggers, sandboxes, and runtime monitoring* • *Malware reverse engineering: techniques and case studies* • *Code obfuscation and anti-reversing techniques* • *Patching and binary modification* • *Reverse engineering of network protocols and communication binaries* • *Reverse engineering of mobile applications (Android/iOS)* • *Tools and frameworks: IDA Pro, Ghidra, Radare2, OllyDbg*
Examination forms	***Exam*** ***Weight*** ***Date*** *Final* *60%* *TBA (to be announced)* *Laboratory* *20%* *every week* *Presentation* *20%* *TBA (to be announced)*
Study and examination requirements	*Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (60%) +Before Exam score will remain the same (40%)*
Reading list	• *Eilam, E., Reversing: Secrets of Reverse Engineering* • *Sikorski, M. & Honig, A., Practical Malware Analysis* • *Dang, D., Practical Reverse Engineering* • *Balaban, V., The IDA Pro Book*

Module designation	***IS 517 - Network Administration***
Semester(s) in which the module is taught	*Year 5, fall semester*
Person responsible for the module	*Lecturer Asim Namazov* *BHOS Bibiheybat Campus ROOM 420* *Asim.namazov@bhos.edu.az* *99412 5210000 ext. 33238*
Language	*English*
Relation to curriculum	*Elective*
Teaching methods	*Lectures, laboratory, presentation*
Workload (incl. contact hours, self-study hours)	*Total workload: 150 h = 102h extracurricular hours + 48h classroom* ***Classroom hours**:* *Lecture: 24h (2 h /week)* *Laboratory: 24h (2 h / week)s* ***Contact hours:*** *Examination preparation, consultation, selfstudy = 8.5 h/ week*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	• *Basic computer networking concepts (TCP/IP, OSI model, subnets)* • *Understanding of operating systems (Windows/Linux)* • *Familiarity with network devices (routers, switches, firewalls)* • *Basic cybersecurity principles (authentication, access control)*
Module objectives/intended learning outcomes	*By the end of the course, students will be able to:* • *Explain the fundamentals of network architecture, protocols, and topologies.* • *Configure and manage network devices such as routers, switches, and firewalls.* • *Implement IP addressing, subnetting, and routing protocols.* • *Monitor network performance and troubleshoot connectivity issues.* • *Apply network security best practices and access control measures.* • *Configure wireless networks and remote access solutions.* • *Document network configurations and maintain network operational procedures.*
Content	• *Introduction to Network Administration and Network Models* • *Network Hardware: Routers, Switches, Hubs, Firewalls* • *TCP/IP Protocol Suite and OSI Model Overview* • *IP Addressing, Subnetting, and VLAN Configuration* • *Routing Protocols: Static and Dynamic (RIP, OSPF)* • *Switching Concepts: STP, VLANs, and Inter-VLAN Routing* • *Wireless Network Configuration and Management* • *Network Services: DHCP, DNS, NAT* • *Firewalls, Access Control, and Network Security Fundamentals*

<table>
<tr><td></td><td>

- *Network Monitoring, Troubleshooting, and Performance Tools*
- *VPNs and Remote Access Technologies*

</td></tr>
<tr><td>Examination forms</td><td>

Exam	***Weight***	***Date***
Final	*60%*	*TBA (to be announced)*
Laboratory	*20%*	*every week*
Presentation	*20%*	*TBA (to be announced)*

</td></tr>
<tr><td>Study and examination requirements</td><td>Student is normally expected to achieve a total mark (preexam score + exam score) of at least 61 to pass. In this case of failure, he/she will be referred or required to repeat the course the following term or year. In the case of failure the student can also be given a chance to retake the exam. Resit Exam score (60%)+Before Exam score will remain the same (40%)</td></tr>
<tr><td>Reading list</td><td>

[1] Andrew S. Tanenbaum & David J. Wetherall, Computer Networks, 5th Edition
[2] William Stallings, Data and Computer Communications, 10th Edition
[3] Todd Lammle, CCNA Study Guide, 7th Edition

</td></tr>
</table>