CYBERSECURİTY MODULE HANDBOOK

Module designation	***CS 101 - Advanced Network Security***
Semester(s) in which the module is taught	*Year 1, fall semester*
Person responsible for the module	*Assoc.Prof. Gunay Abdiyeva-Aliyeva* *BHOS White City Building ROOM 301* *gunay.abdiyeva@bhos.edu.az* *99412 5210000 ext. 33030*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, laboratory, presentation, project*
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)* *Laboratory: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, self-study = 10 h/ week*
Credit points	*6 ECTS*
Required and recommended prerequisites for joining the module	• *Fundamentals of computer networks (OSI, TCP/IP models)* • *IPv4 and IPv6 addressing and subnetting* • *Basic router and switch configuration (Cisco IOS or equivalent)* • *LAN and WAN design principles* • *Basic static and dynamic routing (RIP, OSPF)* • *VLAN configuration and inter-VLAN routing* • *Network security basics (ACLs, authentication, VPN)* • *Wireless networking fundamentals (802.11 standards, AP setup)* • *Basic troubleshooting using network tools and CLI commands* • *Awareness of network services (DHCP, DNS, NTP, SNMP)* • *Basic understanding of virtualization concepts*
Module objectives/intended learning outcomes	• *Illustrate the hierarchical network design model and architecture using the access, distribution, and core layers* • *Troubleshoot Layer 2 connectivity using VLANs and trunking* • *Implement redundant switched networks using Spanning Tree Protocol* • *Troubleshoot link aggregation using Etherchannel* • ***Explain and compare** enterprise routing, switching, and wireless security mechanisms (e.g., VLANs/STP, EIGRP/OSPF, VRRP/HSRP, NAT, 802.11, EAP/PSK).* • ***Analyse** network performance and security risks using monitoring/diagnostic data (SNMP, NetFlow/IPFIX, IP SLA), and **prioritise** risks.* • ***Design and justify** a secure campus segmentation and access-control architecture (L2/L3 segmentation, routing, ACLs, VPN/WAN overlay).*

	• ***Operate, harden, and troubleshoot*** *routed, switched, and wireless infrastructures using contemporary vendor tools and best practice.* • ***Document and present*** *a technical design dossier and incident/troubleshooting log; collaborate effectively in the project team.*
Content	• *Device configuration. Switching concepts. Packet forwarding.* • *Vlans. Inter-vlan routing. Vlan trunks and etherchannel bundles.* • *Spanning tree protocol. Advanced STP tuning.* • *Advanced BGP.* • *DHCPv4. SLAAC and DHCPv6* • *FHRP concepts* • *LAN security concepts* • *Switch security configuration* • *WLAN concepts. WLAN configuration* • *routing concepts. IP services. IP static routing.* • *Wireless infrastructure. Troubleshoot static and default routes.* • *Secure network access control. Network device access control and infrastructure security.*
Examination forms	***Exam*** — ***Weight*** — ***Date*** *Final* — *40%* — *TBA (to be announced)* *Project* — *30%* — *TBA (to be announced)* *Laboratory* — *30%* — *one task 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] Switching, Routing, and Wireless Essentials. Companion Guide (CCNAv7). 2020. Ch.1-2* *[2] CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, 2nd Edition Bradley Edgeworth, Ramiro Garza Rios, David Hucaby, Jason Gooley*

Module designation	***CS 103 - Advanced Cryptography and Data Security***
Semester(s) in which the module is taught	*Year 1, fall semester*
Person responsible for the module	*Lecturer Agha Aghayev* *BHOS White City Building ROOM 301* *agha.aghayev@bhos.edu.az*

	99412 5210000 ext. 33030
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, laboratory, presentation, class tests, midterm*
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)* *Laboratory: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, self-study = 10 h/ week*
Credit points	*6 ECTS*
Required and recommended prerequisites for joining the module	• *Discrete Mathematics (sets, modular arithmetic, number theory)* • *Linear Algebra (matrices, vectors, finite fields)* • *Basic Abstract Algebra (groups, rings, fields)* • *Programming skills (Python, C, or Java)* • *Algorithms and Data Structures* • *Computer Architecture fundamentals (binary operations, bit manipulation)* • *Computer Networks basics (TCP/IP, SSL/TLS, data transmission)* • *Information Security fundamentals (CIA triad, authentication, common attack types)* • *Mathematical Logic and formal reasoning* • *Basic understanding of proofs and pseudocode*
Module objectives/intended learning outcomes	• *Explain foundational cryptography principles (confidentiality, integrity, authenticity), major primitives, and threat models.* • *Analyze and evaluate the security of cryptographic schemes and protocols, identifying vulnerabilities and attack vectors.* • *Design, implement, and evaluate cryptographic solutions (symmetric/asymmetric encryption, hashing, signatures, key exchange) to meet application requirements.* • *Investigate contemporary research topics (e.g., zero-knowledge, side-channel attacks, protocol proofs) using appropriate scholarly methods.* • *Apply advanced techniques such as PKI, lattice-based/post-quantum cryptography, and homomorphic encryption, selecting methods appropriate to constraints.* • *Assess compliance, legal, and ethical considerations (e.g., GDPR data protection, export controls, NIST/ISO/ETSI standards) when deploying cryptography.* • *Communicate technical analyses and results effectively in written reports and oral presentations, and collaborate productively on team-based tasks.* • *Adapt to emerging technologies and threats, comparing new cryptographic primitives/protocols and articulating migration paths (e.g., to PQC).*
Content	• Introduction to Cryptography and Security Objectives

	• Mathematical Background (modular arithmetic, finite fields, number theory) • Symmetric-Key Cryptography: Stream and Block Ciphers • DES, AES, and modern block cipher structures • Asymmetric Cryptography: Public-Key Systems • RSA, ElGamal, and Discrete Logarithm Systems • Cryptographic Hash Functions and Message Authentication Codes (MAC) • Digital Signatures and Public Key Infrastructure (PKI) • Key Exchange and Management Protocols (e.g., Diffie–Hellman, TLS overview) • Cryptanalysis and Attack Methods (brute-force, differential, linear, side-channel) • Modern Cryptographic Paradigms • Zero-Knowledge Proofs, Lattice-Based Cryptography, Homomorphic Encryption • Quantum-Resistant and Privacy-Preserving Cryptography • Post-quantum schemes, privacy homomorphism, and secure multiparty computation
Examination forms	***Exam*** — ***Weight*** — ***Date*** *Final* — *40%* — *TBA (to be announced)* *Midterm* — *30%* — *6th week of the semester* *Presentation* — *20%* — *TBA (to be announced)* *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] Paar, C., & Pelzl, J. (2010). Understanding cryptography (Vol. 1). Springer-Verlag Berlin Heidelberg.* *[2] Katz, J., & Lindell, Y. (2007). Introduction to modern cryptography: principles and protocols. Chapman and hall/CRC.* *[3] Lecture notes of Vinod https://people.csail.mit.edu/vinodv/CS294/lecturenotes.pdf* *[4] Peikert, C. (2016). A decade of lattice cryptography. Foundations and trends® in theoretical computer science, 10(4), 283-424.*

Module designation	***CS 105 - Advanced Ethical Hacking***
Semester(s) in which the module is taught	*Year 1, fall semester*
Person responsible for the module	*Lecturer Emil Farzaliyev* *BHOS White City Building ROOM 301* *emil.farzaliyev@bhos.edu.az*

	99412 5210000 ext. 33030
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, laboratory, presentation, project*
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)* *Laboratory: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, self-study = 10 h/ week*
Credit points	*6 ECTS*
Required and recommended prerequisites for joining the module	• *Fundamentals of computer networks (OSI and TCP/IP models)* • *IPv4 and IPv6 addressing, subnetting, and routing basics* • *Basic understanding of network devices (switches, routers, firewalls)* • *Knowledge of operating systems (Windows and Linux) and command-line tools* • *Basic skills in system administration and file permissions* • *Understanding of common network protocols (HTTP, DNS, FTP, SMTP, etc.)* • *Awareness of security concepts (confidentiality, integrity, availability)* • *Familiarity with network security mechanisms (firewalls, IDS/IPS, VPNs)* • *Basic understanding of web technologies and databases* • *Introduction to cryptography (encryption, hashing, digital signatures)* • *Familiarity with virtualization and lab environments (e.g., VMware, VirtualBox)* • *Basic knowledge of cybersecurity threats and incident response principles*
Module objectives/intended learning outcomes	• *Apply Ethical Hacking Concepts: Demonstrate an understanding of ethical hacking principles and concepts, including its role in ensuring information security.* • *Perform reconnaissance & threat modelling using OSINT and network discovery to prioritise attack paths.* • *Execute vulnerability scanning & verification (tuning tools, reducing false positives, manual validation).* • *Exploit and escalate on Windows/Linux and web stacks; maintain and safely remove access; propose mitigations.* • *Assess malware-style TTPs (credential theft, persistence, C2, evasion) and recommend defensive controls.* • *Secure wireless, mobile, IoT and cloud-adjacent surfaces with appropriate attack/defence techniques.* • *Produce professional reporting & communicate findings (risk, impact, PoC, remediation, re-test plan).* • *Track emerging threats & adapt toolchains (exploit frameworks, scripts, containers) to new vulnerabilities.*

<table>
<tr><td>Content</td><td>• Ethics, law, and rules of engagement (contracts, consent, scope, reporting, chain of custody)

• Pentest methodology (PTES/OSSTMM/NIST 800-115), project planning, risk & safety

• Reconnaissance & OSINT (footprinting, attack surface mapping, threat modelling)

• Scanning & enumeration (network/service discovery, banners, fingerprinting, vuln scanning & validation)

• Exploitation & post-exploitation (Windows/Linux privilege escalation, lateral movement, cleanup)

• Web application security (OWASP Top 10, auth/session, SQLi/XSS/XXE/SSRF; secure coding mitigations)

• Wireless & IoT security (EAP/PSK, WLC, BLE/802.11 attacks, device hardening)

• Mobile & client-side attacks (Android/iOS basics, storage, instrumentation; phishing & social engineering)

• Malware-style techniques & evasion (persistence, credential dumping, C2, sandbox anti-analysis—blue-team countermeasures)

• Cloud & container attack surfaces (intro) (common misconfigs; shared-responsibility; basic hardening)

• DoS/availability & network countermeasures (rate-limiting, WAF/IPS rules of engagement)

• Reporting & presentation (risk, exploit narrative, PoC, remediation plan, re-test)</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>Laboratory</td><td>30%</td><td>one lab per week</td></tr><tr><td>Project</td><td>30%</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 (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] Certified Ethical Hacking (CEH) v12. EC-Council. 2022
[2] https://www.eccouncil.org/train-certify/certified-ethical-hacker-ceh/</td></tr>
</table>

Module designation	***CS 107 - Incident Response***
Semester(s) in which the module is taught	*Year 1, fall semester*
Person responsible for the module	*Lecturer Safura Isayeva* *BHOS White City Building ROOM 301* *safura.isayeva@bhos.edu.az* *99412 5210000 ext. 33030*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, laboratory, presentation, project, quiz*
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)* *Laboratory: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, self-study = 10 h/ week*
Credit points	*6 ECTS*
Required and recommended prerequisites for joining the module	• *Fundamentals of computer networks (OSI and TCP/IP models)* • *Basic understanding of network devices and architectures (routers, switches, firewalls)* • *Knowledge of operating systems (Windows and Linux) administration and file systems* • *Awareness of common cybersecurity concepts (threats, vulnerabilities, exploits, risk management)* • *Familiarity with security tools such as antivirus, IDS/IPS, and SIEM systems* • *Understanding of basic network protocols (HTTP, DNS, SMTP, FTP, etc.)* • *Basic knowledge of digital forensics principles and evidence handling* • *Awareness of malware types, attack vectors, and social engineering techniques* • *Basic experience with log analysis and network monitoring* • *Familiarity with security policies, regulatory frameworks, and compliance standards*
Module objectives/intended learning outcomes	• *Explain the goals, roles, and phases of the incident response lifecycle (prep, detect/analysis, contain/eradicate/recover, post-incident).* • *Triage and analyze alerts, logs, and indicators to determine incident scope, impact, and priority.* • *Design and execute containment, eradication, and recovery plans appropriate to the incident type and business constraints.* • *Use modern SOC tooling (SIEM, EDR, packet analysis, threat intel feeds, SOAR playbooks) to investigate and respond.* • *Document evidence and preserve chain of custody to support potential legal or disciplinary proceedings.*

	• *Communicate findings, status, and recommendations clearly to both technical teams and management; participate effectively in blue-/red-team exercises.* • *Reflect on lessons learned and update runbooks/playbooks, adapting to emerging threats and technologies.*
Content	*Introduction to Incident Response* • *Definition, scope, and objectives of incident response* • *Roles and responsibilities within an IR team* • *Incident classification, severity levels, and communication flow* *Preparation Phase* • *Incident response policies, procedures, and playbooks* • *Asset inventory, baselines, and logging infrastructure* • *Setting up monitoring tools (SIEM, IDS/IPS, EDR)* • *Building and training Computer Security Incident Response Teams (CSIRT)* *Identification and Initial Response* • *Recognizing indicators of compromise (IoCs)* • *Alert triage, validation, and escalation procedures* • *Log analysis and correlation using SIEM platforms* • *Coordination between detection and response teams* *Containment, Eradication, and Recovery* • *Containment strategies (short-term vs. long-term)* • *Malware removal and system sanitization* • *System restoration and verification of service integrity* • *Post-recovery validation and lessons learned* *Investigation and Analysis* • *Evidence collection and preservation* • *Digital forensics fundamentals and chain of custody* • *Root cause analysis and threat attribution* • *Tools for endpoint and network investigations* *Communication and Coordination* • *Internal and external communication protocols* • *Stakeholder reporting and incident documentation* • *Incident severity communication matrix and reporting templates* *Post-Incident Activities* • *Reporting and documentation standards* • *Lessons learned meetings and improvement plans* • *Updating IR playbooks and response policies* • *Metrics and KPIs for IR effectiveness evaluation* *Specialized Incident Domains* • *Cloud Incident Response: log sources, CSP coordination, shared responsibility model*

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

IoT and OT Incidents: isolation, containment, and safety priorities
Identity-Related Incidents: account compromise and privilege escalation detection

Threat Hunting and Automation

Proactive hunting using hypotheses and threat intelligence
Integration of MITRE ATT&CK framework
Use of SOAR (Security Orchestration, Automation, and Response) platforms
Developing and maintaining automated playbooks

Red Team vs. Blue Team Exercises

Simulating attacks and responses
Building defensive detection rules and countermeasures
Measuring readiness and continuous improvement

Course Summary and Review

Integration of all phases in a simulated incident scenario
Group project and final assessment review

</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>20%</td><td>one lab per week</td></tr>
<tr><td>Quiz</td><td>10%</td><td>every 3 week</td></tr>
<tr><td>Project</td><td>10%</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 (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>[1] R.Brown, S.J. Roberts Intelligence-Driven Incident Response, 2nd Edition. 2023
[2] https://www.first.org/resources/guides/</td></tr>
</table>

Module designation	***CS 109 - Machine Learning***
Semester(s) in which the module is taught	*Year 1, fall semester*
Person responsible for the module	*Assoc.Prof.Leyla Muradkhanli* *BHOS White City Building ROOM 301* *leyla.muradkhanli@bhos.edu.az* *99412 5210000 ext. 33030*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, laboratory, presentation, project, quiz*
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)* *Laboratory: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, self-study = 10 h/ week*
Credit points	*6 ECTS*
Required and recommended prerequisites for joining the module	• *Fundamentals of programming (preferably Python)* • *Basic understanding of data structures and algorithms* • *Knowledge of linear algebra (vectors, matrices, operations)* • *Understanding of calculus concepts (derivatives, gradients)* • *Basic statistics and probability theory* • *Familiarity with data analysis and visualization techniques* • *Awareness of database concepts and data handling (e.g., CSV, SQL)* • *Introductory knowledge of artificial intelligence concepts* • *Experience with numerical computing tools (e.g., NumPy, pandas, matplotlib)*
Module objectives/intended learning outcomes	• *Demonstrate a solid understanding of the fundamental concepts, principles, and mathematical foundations of machine learning, including supervised, unsupervised, and reinforcement learning paradigms.* • *Preprocess, clean, and transform real-world datasets using statistical and computational techniques to ensure data quality and readiness for model development.* • *Design, implement, and train machine learning models using modern tools and frameworks (e.g., Scikit-learn, PyTorch, TensorFlow) for solving applied problems in cybersecurity and data analysis.* • *Evaluate and compare machine learning models using standard performance metrics and apply optimization techniques to improve accuracy, generalization, and efficiency.*

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

- *Interpret and explain model behavior using explainable AI techniques, ensuring fairness, accountability, and transparency in decision-making.*
- *Integrate machine learning methodologies into cybersecurity applications such as intrusion detection, anomaly detection, and threat prediction to enhance system resilience.*
- *Work collaboratively on research-driven projects, communicate findings effectively through reports and presentations, and apply ethical considerations in AI system design.*

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

- *Basic Concepts in Machine Learning*
- *Data Preparation and Processing*
- *Regression Linear Regression*
- *Classification Logistic Regression*
- *Classification k-Nearest Neighbors (k-NN) algorithm*
- *Classification Decision Trees Random Forests*
- *Classification Support Vector Machines (SVM)*
- *Clustering. k-Means clustering*
- *Dimensionality Reduction*
- *Neural Networks*
- *Applications of Machine Learning*

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

Exam	***Weight***	***Date***
Final	*40%*	*TBA (to be announced)*
Assignment	*30%*	*every week*
Quiz	*15%*	*6th week of semester*
Project	*15%*	*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] Understanding Machine Learning: From Theory to Algorithms by Shai Shalev-Shwartz and Shai Ben-David, Cambridge University Press, 2014.

[2] Machine Learning with PyTorch and Scikit-Learn : Develop machine learning and deep learning models with Python by Sebastian Raschka, Yuxi (Hayden) Liu, Vahid Mirjalili, Packt Publishing, 2022.

[3] Machine Learning. An Algorithmic Perspective, Stephen Marsland, Second edition, CRC Press, 2015.

[4] Introduction to Machine Learning with Python by Andreas C. Müller, Sarah Guido, O'Reilly Media, 2016.

[5] Neural Networks and Deep Learning, Charu C. Aggarwal, Springer, 2018.

[6] D. Barber, Bayesian Reasoning and Machine Learning, Cambridge University Press 2012.

[7] Christopher M. Bishop, Pattern recognition and Machine Learning, Springer, 2006.

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

	[8] Mathematics for Machine Learning by Marc Peter Deisenroth, A. Aldo Faisal, and Cheng Soon Ong, Cambridge University Press, 2020. *[9] K.P. Murphy, Machine Learning: a probabilistic perspective, MIT Press, 2012.*

Module designation	***CS 102 - Advanced Mobile Security***
Semester(s) in which the module is taught	*Year 1, spring semester*
Person responsible for the module	*Lecturer Samir Fataliyev* *BHOS White City Building ROOM 301* *samir.fataliyev@bhos.edu.az* *99412 5210000 ext. 33030*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, laboratory, presentation, project, quiz*
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)* *Laboratory: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, self-study = 10 h/ week*
Credit points	*6 ECTS*
Required and recommended prerequisites for joining the module	• *Programming fundamentals (Java/Kotlin or Swift) and basic scripting (e.g., Python/Bash)* • *Computer networks (HTTP/HTTPS, TLS, Wi-Fi/Bluetooth basics)* • *Operating systems concepts; basic Android and iOS user-level familiarity* • *Information security fundamentals (CIA, authn/authz, access control, hashing, encryption)* • *Databases & data handling (SQL/NoSQL, local storage)*
Module objectives/intended learning outcomes	• *Explain platform security models for Android and iOS (sandboxing, permissions, app signing, secure boot, keystore/keychain).* • *Analyse mobile threats and vulnerabilities (app, device, network, baseband) using OWASP MASVS/MSTG and risk-assessment methods.* • *Design and implement secure solutions for mobile apps (secure storage, auth, session mgmt, TLS/cert-pinning, API hardening).* • *Select and use appropriate tools and techniques (MobSF, Frida, Burp Suite, drozer, adb/Xcode instruments) to test, debug, and verify mobile security controls.* • *Communicate security findings with clear technical documentation and a short team presentation (vuln reports, remediation plans).* • *Adapt to emerging trends (e.g., RASP, passkeys/WebAuthn, eSIM, mobile EDR/MDM) and reflect on privacy/ethics and relevant policies.*
Content	• *Mobile Security Foundations: threat landscape, MASVS/MSTG, attacker models* • *Platform Security Models: Android/iOS architecture, sandboxing, permissions, app signing, secure boot, keystore/keychain*

	• *Secure Data Storage: key management, encrypted storage, biometrics, backups* • *Authentication & Session Management: OAuth2/OIDC, tokens, refresh/rotation, device binding, WebAuthn/passkeys* • *Network & Transport Security: TLS, certificate pinning, secure sockets, DoH/DoT, VPN; Wi-Fi, Bluetooth, NFC risks* • *API & Backend Security for Mobile: input validation, rate limiting, abuse prevention, anti-automation, backend RBAC/ABAC* • *Secure Coding for Android/iOS: common pitfalls, secure configs, logging, secrets handling, build/signing pipelines* • *App Hardening & Resilience: jailbreak/root detection, code obfuscation, RASP basics, anti-debugging* • *Mobile Security Testing Tools: MobSF, Frida/Objection, drozer, Burp, adb/Xcode instruments; test plan design* • *Mobile Malware & Reverse Engineering (intro): packing, hooking, static/dynamic triage* • *Mobile Device, MDM & Enterprise Controls: device compliance, EDR/MDM, BYOD risks* • *Privacy, Policy, and Ethics: permissions minimisation, telemetry, legal/ethical testing guidelines* • *Case Study & Mini-Project: threat modelling + secure re-design of a mobile app; written report & presentation* • *Review & Emerging Trends: RASP advances, eSIM, secure elements/TEE, passkeys, app attestation*
Examination forms	***Exam*** ***Weight*** ***Date*** *Final* *70%* *TBA (to be announced)* *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 (70%) +Before Exam score will remain the same (30%)*
Reading list	***Textbooks:*** *[1] "Mobile Security and Privacy: Advances, Challenges and Future Research Directions" by Man Ho Au and Raymond Choo* *[2] OWASP Mobile Security Project* *[3] Apple's iOS Security Guide* *[4] NIST Special Publication on Mobile Device Security* *[5] "Mobile Application Security" by Himanshu Dwivedi, Chris Clark, and David Thiel* *[6] "Android Security Internals: An In-Depth Guide to Android's Security Architecture"* *[7] "Practical Mobile Forensics" by Heather Mahalik, Satish Bommisetty, and Rohit Tamma* ***Papers:*** *[5] "Android Security: A Survey of Issues, Malware Penetration, and Defenses" Authors: Yajin Zhou and Xuxian Jiang*

	[6] "Security Challenges in the iOS Operating System" Authors: Michael Rogers and Saleh Ibrahim

Module designation	***CS 104 - Cybersecurity Law, Policy, and Ethics***
Semester(s) in which the module is taught	*Year 1, spring semester*
Person responsible for the module	*Nigar Guliyeva*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, laboratory, presentation, project, quiz*
Workload (incl. contact hours, self-study hours)	*Total workload: 120 h = 84 h extracurricular hours + 36 h classroom* ***Classroom hours**:* *Lecture: 24 h (2 h /week)* *Laboratory: 12 h (1 h / week)* ***Contact hours:*** *Examination preparation, consultation, self-study = 7 h/ week*
Credit points	*4 ECTS*
Required and recommended prerequisites for joining the module	• *Basic understanding of information and communication technologies (ICT)* • *Familiarity with fundamental cybersecurity and data protection concepts* • *Awareness of how the Internet and digital platforms function (network, data flow, digital identity)* • *General knowledge of international and national legal systems* • *Understanding of key concepts in information security and privacy* • *Awareness of emerging technologies (AI, Big Data, IoT) and their social implications* • *Basic research and academic writing skills for analyzing laws and regulations*
Module objectives/intended learning outcomes	• Explain the key concepts and principles of cybersecurity law, policy, and ethics at both national and international levels. • Analyze the legal distinctions between general and special categories of personal data and their implications for data protection. • Evaluate the structure and objectives of Internet governance regimes and their importance in global cybersecurity policymaking. • Examine the influence of major technology companies on law, democracy, and digital diplomacy. • Compare and contrast international and regional cybersecurity regulations (e.g., GDPR, AI Act, NIS2, Azerbaijan law). • Critically assess emerging technologies such as AI, Big Data, and IoT from a legal and ethical perspective. • Apply legal reasoning to real-world cybersecurity cases involving privacy breaches, intellectual property, and e-commerce. • Present well-structured legal and policy analyses, and collaborate effectively within multidisciplinary teams to address emerging IT law challenges.

Content	• *Information Security and Privacy* • *Role of High-Tech Companies* • *Digital Signature* • *Artificial Intelligence (AI)* • *E-Commerce Law* • *Intellectual Property Law and Algorithms* • *Human Rights and Algorithms* • *Critical Infrastructure Protection* • *Cyber Crimes* • *Azerbaijani Criminal Code on Cybercrime* • *Course Evaluation*
Examination forms	***Exam*** ***Weight*** ***Date*** *Final* *50%* *TBA (to be announced)* *Quiz* *30%* *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 (70%)+Before Exam score will remain the same (30%)*
Reading list	*[1] Kuner, C. (2020). Transborder Data Flows and Data Privacy Law. Oxford University Press.* *[2] Lloyd, I. (2021). Information Technology Law. 9th Edition, Oxford University Press.* *[3] Kerr, O. S. (2022). Computer Crime Law. West Academic Publishing.* *[4] Greenleaf, G., & Waters, N. (2023). Global Data Privacy Laws 2023: 152 National Laws & DPAs. Privacy Laws & Business.*

Module designation	***CS 106 - Cyber Threat Intelligence***
Semester(s) in which the module is taught	*Year 1, spring semester*
Person responsible for the module	*Assoc.Prof. Gunay Abdiyeva-Aliyeva* *BHOS White City Building ROOM 301* *gunay.abdiyeva@bhos.edu.az* *99412 5210000 ext. 33030*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, laboratory, presentation, project*
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, self-study = 8.5 h/ week*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	• *Fundamentals of computer networks (OSI/TCP-IP), subnetting, routing/switching basics* • *Operating systems (Windows & Linux), command-line skills* • *Core cybersecurity concepts (CIA, threats, vulns, exploits, risk)* • *Network protocols (DNS, HTTP/HTTPS, SMTP, etc.)* • *Intro to digital forensics & incident response (logs, evidence handling)* • *Awareness of malware types and common TTPs* • *Basic scripting or data analysis (Python preferred)*
Module objectives/intended learning outcomes	• *Explain the role, scope, and vocabulary of CTI and the Intelligence Life Cycle.* • *Plan and execute ethical collection activities (OSINT, technical sources) aligned to stakeholder requirements.* • *Analyze indicators and behaviors (IOCs/IOBs) and attribute activity using structured analytic techniques.* • *Use and operationalize industry frameworks and standards (MITRE ATT&CK, D3FEND, STIX/TAXII).* • *Model threats and assess risk; propose courses of action (COAs) for SOC/IR and leadership.* • *Produce actionable intelligence products (written briefs, visuals, and oral updates) tailored to different audiences.* • *Automate parts of the CTI workflow (enrichment, correlation, sharing) with common tools/APIs or scripts.* • *Interpret legal, ethical, and privacy constraints on collection, processing, and sharing of intelligence.* • *Collaborate effectively with SOC/Blue Team/IR to integrate CTI into operations and measure impact.*
Content	• *Introduction to Cyber Threat Intelligence (CTI)*

	• *Threat Landscape and Cyber Kill Chain* • *Types of Threat Actors and Motivations* • *Intelligence Lifecycle: Planning, Collection, Analysis, Dissemination* • *Data Sources for Threat Intelligence* • *Open-Source Intelligence (OSINT)* • *Technical Intelligence: Indicators of Compromise (IoCs)* • *Tactical, Operational, and Strategic Intelligence Levels* • *Threat Modeling and Analysis Techniques* • *Use of Frameworks: MITRE ATT&CK, STIX, TAXII* • *Malware and APT Analysis Fundamentals* • *Threat Intelligence Sharing and Collaboration* • *Automation and Tools in Threat Intelligence* • *Legal and Ethical Considerations in Threat Intelligence* • *Case Studies and Real-World Applications* • *Course Review and Final Assessment*
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	*[1] FOR578.1: Mike Cloppert, Chris Sperry, and Robert M. Lee. FOR578: Cyber Threat Intelligence* *[2] Cyber Threat Intelligence*

Module designation	***CS 108 - Advanced IoT Security***
Semester(s) in which the module is taught	*Year 1, spring semester*
Person responsible for the module	*PhD, Elshan Rahimov* *BHOS White City Building ROOM 301* *elshan.rahimov@bhos.edu.az* *99412 5210000 ext. 33030*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, laboratory, presentation, project*
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, self-study = 8.5 h/ week*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	• *Basic understanding of computer networks and communication protocols* • *Fundamental knowledge of electronics and embedded systems* • *Familiarity with programming concepts (e.g., Python, C, or Java)* • *Basic knowledge of sensors, actuators, and microcontrollers (e.g., Arduino, Raspberry Pi)* • *Understanding of data collection and processing principles* • *Awareness of cybersecurity fundamentals and data privacy concepts* • *Basic analytical and problem-solving skills for technical systems*
Module objectives/intended learning outcomes	• *Demonstrate advanced understanding of IoT system components, architectures, and communication models used in telematics and cyber-physical environments.* • *Analyse and evaluate security challenges in IoT ecosystems, including authentication, authorization, and secure data exchange mechanisms.* • *Design secure and resilient IoT architectures that integrate safety, privacy, and performance considerations, applying secure-by-design and DevSecOps principles.* • *Make evidence-based decisions under uncertainty, considering legal, ethical, societal, and operational implications of IoT system deployment.* • *Conduct reproducible laboratory experiments involving IoT devices, threat simulations, and vulnerability testing using standard security frameworks.* • *Communicate technical findings effectively through written laboratory reports, presentations, and collaborative projects.*
Content	• *IoT and Telematics — definitions, architectures, and properties* • *IoT in practice and daily life*

	• *Measurement systems in telematics* • *Data exchange and protocols in IoT (MQTT, CoAP, HTTPS)* • *Security challenges in IoT: authentication, key management, encryption* • *Origins of errors, measurement accuracy, and trust models* • *IoT in various life areas (healthcare, transportation, smart cities)* • *GPRS, LPWAN, and 5G technologies* • *Applying telematics devices in practice* • *Automation systems and fleet management using IoT* • *Emerging topics: zero-trust IoT, AI-driven anomaly detection, digital twin security*
Examination forms	***Exam*** ***Weight*** ***Date*** *Final* *60%* *TBA (to be announced)* *Laboratory* *40%* *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]IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing,DavidHanis, Cisco Press; 1 edition, 2017, 575 pages.* *[2] Enterprise IoT: Strategies and Best Practices for Connected Products and Services, Dirk Slama, Frank Puhlmann , Jim Morrish, Rishi M Bhatnagar, O'Reilly Media, 2015, 492 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] Designing Connected Products: UX for the Consumer Internet of Things 1st Edition, Claire Rowland, Elizabeth Goodman, Martin Charlier, Ann Light, Alfred Lui,O'Reilly Media, 2015, 726 pages.* *[6] Abusing the Internet of Things: Blackouts, Freakouts, and Stakeouts, 1st Edition,NiteshDhanjani, O'Reilly Media, 2015, 296 pages.*

Module designation	***CS 110 Advanced Penetration Testing***
Semester(s) in which the module is taught	*Year 1, spring semester*
Person responsible for the module	*Assoc.Prof. Gunay Abdiyeva-Aliyeva* *BHOS White City Building ROOM 301* *gunay.abdiyeva@bhos.edu.az* *99412 5210000 ext. 33030*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, laboratory, presentation, project*
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, self-study = 8.5 h/ week*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	• *Completion of Ethical Hacking or Information Security Fundamentals course* • *Solid understanding of networking concepts and TCP/IP* • *Familiarity with operating systems (Windows, Linux)* • *Experience with penetration testing tools and frameworks (Nmap, Metasploit, Burp Suite, OWASP ZAP)* • *Basic programming/scripting skills in Python, Bash, or PowerShell*
Module objectives/intended learning outcomes	• *Gain technical proficiency in using advanced penetration testing tools and methodologies to identify and exploit vulnerabilities.* • *Develop an adversarial mindset and anticipate real-world attack tactics, techniques, and procedures (TTPs).* • *Perform zero-day exploitation and assess emerging vulnerabilities using ethical frameworks.* • *Conduct post-exploitation analysis to evaluate security impact and lateral movement.* • *Carry out risk assessment and reporting of vulnerabilities with prioritization based on criticality.* • *Produce professional penetration testing reports and communicate findings effectively to stakeholders.* • *Apply legal and ethical considerations in all testing phases, ensuring compliance with organizational and national standards.* • *Collaborate in multidisciplinary teams to perform simulated cyberattacks and security audits.*
Content	***Introduction and Lab Setup*** • *Virtual lab design and documentation standards* • *Ethical hacking principles and penetration testing methodology*

	Information Gathering & Scanning • *Network discovery (Nmap, Netdiscover)* • *Vulnerability scanning (OpenVAS, Nessus, Nikto)* • *Banner grabbing and reconnaissance techniques* ***Exploitation and Privilege Escalation*** • *Exploiting web, network, and system vulnerabilities* • *Reverse shells, persistence mechanisms* • *Privilege escalation in Linux and Windows environments* ***Post-Exploitation and Lateral Movement*** • *Maintaining access and pivoting* • *Credential harvesting and evidence collection* • *Post-exploitation analysis and cleanup procedures* ***Application and Cloud Testing*** • *OWASP Top 10 testing framework* • *Web application testing methodologies* • *Cloud environment (AWS, Azure) penetration testing basics* ***Social Engineering and Physical Security Testing*** • *Phishing simulation and human-factor exploitation* • *Awareness of ethical constraints in human-based testing* ***Reporting and Documentation*** • *Comprehensive penetration testing report writing* • *Risk scoring, vulnerability prioritization (CVSS)* • *Communicating results to technical and non-technical audiences* ***Legal and Ethical Frameworks*** • *Compliance standards: ISO 27001, GDPR, NIST SP 800-115* • *Laws and ethics in cybersecurity operations* ***Continuous Improvement and Final Project*** • *Automation in penetration testing (scripts and CI/CD pipelines)* • *Final project and course review*
Examination forms	***Exam*** ***Weight*** ***Date*** *Final* *40%* *TBA (to be announced)* *Laboratory* *30%* *every 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] Lee Allen. Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide* *[2] Wil Allsopp. Advanced Penetration Testing*

Module designation	***CS 201 - Advanced Blockchain Security***
Semester(s) in which the module is taught	*Year 2, fall semester*
Person responsible for the module	*Lecturer Nihad Alili* *BHOS White City Building ROOM 301* *nihad.elili@bhos.edu.az* *99412 5210000 ext. 33030*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, laboratory, presentation, quiz*
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)* *Laboratory: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, self-study = 10 h/ week*
Credit points	*6 ECTS*
Required and recommended prerequisites for joining the module	• *Fundamental understanding of blockchain technology and distributed ledger systems* • *Basic cryptography concepts (hash functions, digital signatures, public/private-key cryptography)* • *Familiarity with smart contracts and decentralized applications (dApps)* • *Knowledge of consensus mechanisms (PoW, PoS etc.)* • *Basic understanding of cybersecurity principles and common attack vectors* • *Programming or scripting experience (e.g., Solidity, Python)*
Module objectives/intended learning outcomes	• *Demonstrate a deep understanding of cryptographic foundations such as hash functions, digital signatures, and elliptic curve cryptography, and explain how these mechanisms ensure the integrity, authenticity, and confidentiality of blockchain transactions.* • *Identify and analyze major security vulnerabilities within blockchain ecosystems, including consensus-level, network-level, and smart-contract-related threats, and assess their potential impact on decentralized platforms.* • *Critically evaluate the security and resilience of various consensus mechanisms such as Proof of Work, Proof of Stake, and Delegated Proof of Stake, recognizing their strengths, weaknesses, and susceptibility to attacks like Sybil, 51 %, and selfish mining.* • *Design and implement technical countermeasures against common blockchain-specific attacks, including double-*

	spending, eclipse, and front-running, while validating their efficiency through experiments or simulations. • *Detect and mitigate smart-contract vulnerabilities such as reentrancy, integer overflow, and access-control flaws, applying secure-coding principles, auditing methodologies, and testing frameworks.* • *Apply advanced privacy-preserving methods, including zero-knowledge proofs (ZK-SNARKs), ring signatures, and confidential transactions, to enhance data anonymity and user privacy in decentralized systems.* • *Examine the security challenges in decentralized finance (DeFi) environments, including flash-loan and oracle manipulation attacks, and develop robust defense and mitigation strategies.* • *Understand and evaluate scalability and security trade-offs in blockchain systems by analyzing approaches like sidechains, sharding, and state channels.* • *Demonstrate awareness of legal, ethical, and regulatory aspects of blockchain technologies, including GDPR, AML/KYC compliance, and policy frameworks, and discuss their implications for secure blockchain deployment and governance.*
Content	• *Introduction to Blockchain Security* • *Cryptography in Blockchain* • *Consensus Mechanisms and Security* • *Smart Contracts and Security* • *Decentralized Applications (dApps) Security* • *Blockchain Attacks – Part 1* • *Blockchain Attacks – Part 2* • *Blockchain Privacy and Anonymity* • *Regulatory and Compliance Issues in Blockchain Security* • *Security in Decentralized Finance (DeFi)* • *Blockchain Scalability and Security* • *Future Trends in Blockchain Security*
Examination forms	***Exam*** ***Weight*** ***Date*** *Final* *40%* *TBA (to be announced)* *Quiz* *30%* *every 3 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	*[1] Andreas M. Antonopoulos - Mastering Bitcoin Programming the Open Blockchain-O'Reilly Media (2017)* *[2] Imran Bashir - Mastering Blockchain (2017, Packt Publishing)*

Module designation	***CS 203 - Secure Software Development and Quality Assurance***
Semester(s) in which the module is taught	*Year 2, fall semester*
Person responsible for the module	*Lecturer Elnur Jafarli* *BHOS White City Building ROOM 301* *elnur.jafarli@bhos.edu.az* *99412 5210000 ext. 33030*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, laboratory, presentation, quiz*
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)* *Laboratory: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, self-study = 10 h/ week*
Credit points	*6 ECTS*
Required and recommended prerequisites for joining the module	• *Basic knowledge of software development and programming concepts.* • *Familiarity with common web technologies and protocols (e.g., HTTP, HTTPS).*
Module objectives/intended learning outcomes	• *Gain an in-depth understanding of secure software development methodologies and their integration within the Software Development Life Cycle (SDLC) to ensure resilience and maintainability of applications.* • *Identify, analyze, and mitigate common software vulnerabilities through secure coding practices, threat modeling, and systematic risk assessment aligned with modern cybersecurity frameworks.* • *Apply encryption, authentication, and integrity mechanisms in software systems to protect sensitive data and ensure confidentiality, availability, and accountability of software assets.* • *Develop and implement secure architectures by applying design principles such as least privilege, zero trust, and defense-in-depth to build robust and scalable software systems.* • *Utilize automated security testing and continuous integration pipelines to detect and remediate vulnerabilities throughout the development process, ensuring proactive security assurance .* • *Conduct comprehensive static and dynamic code analyses to validate software reliability, compliance, and security against industrial standards and organizational policies.* • *Collaborate effectively in cross-functional development and security teams to address software vulnerabilities, ensure code quality, and meet compliance and regulatory requirements.*

	• *Demonstrate professional ethics, accountability, and responsibility in software assurance processes, ensuring adherence to legal, ethical, and security standards in secure software engineering*
Content	• *Introduction to Secure Software Development* • *Software Vulnerabilities* • *Threat Modeling and Risk Management* • *Cryptography in Software Development* • *Input Validation and Output Encoding* • *Secure Coding Best Practices* • *Software Testing and Security Assurance* • *Automated Security Testing Tools* • *Quality Assurance in Secure Software Development* • *Incident Response and Secure Maintenance* • *Secure Software Development Case Studies and Industry Practices*
Examination forms	***Exam*** ***Weight*** ***Date*** *Final* *25%* *TBA (to be announced)* *Quiz* *20%* *every 3 week* *Project* *25%* *TBA (to be announced)* *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 (25%)+Before Exam score will remain the same (75%)*
Reading list	• *"The Web Application Hacker's Handbook" by Dafydd Stuttard &Marcus Pinto A comprehensive guide on web application security, vulnerabilities, and attack methodologies.* • *"Software Security: Building Security In" by Gary McGraw Focuses on how to build security into every aspect of the software development process.* • *"The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities" by Mark Dowd, John McDonald, and Justin Schuh An in-depth guide to identifying vulnerabilities in software and assessing risk.*

Module designation	***CS 205 - Digital Forensics***
Semester(s) in which the module is taught	*Year 2, fall semester*
Person responsible for the module	*Assoc.Prof. Gunay Abdiyeva-Aliyeva* *BHOS White City Building ROOM 301* *gunay.abdiyeva@bhos.edu.az* *99412 5210000 ext. 33030*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, laboratory, presentation, quiz*
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)* *Laboratory: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, self-study = 10 h/ week*
Credit points	*6 ECTS*
Required and recommended prerequisites for joining the module	• *Basic understanding of computer systems and operating systems (Windows, Linux, MacOS)* • *Fundamentals of networking and network protocols* • *Introductory knowledge of cybersecurity concepts* • *Awareness of malware types and threats* • *Basic familiarity with programming or scripting is advantageous*
Module objectives/intended learning outcomes	• *Explain how to prepare and plan a digital forensics investigation by following a systematic, standardized approach consistent with professional and legal requirements.* • *Analyze how advances in computer and communication technologies have influenced the development, complexity, and evolving nature of cybercrime.* • *Determine appropriate sources of digital evidence, describe methods of data collection, and apply proper techniques for identifying, preserving, and documenting forensic data.* • *Explain standard operating procedures and protocols used during forensic analysis, including acquisition, verification, and chain-of-custody maintenance.* • *Utilize modern digital forensic tools and software to examine different types of digital evidence, such as disk images, memory captures, and log files, in diverse cybercrime scenarios.* • *Apply current industry practices to data recovery, duplication, and analysis, including handling of anti-forensic and obfuscation techniques.* • *Perform forensic investigations on multiple operating systems (Windows, Linux, macOS) and network environments, demonstrating competence in platform-specific forensic techniques.* • *Investigate and interpret evidence from various digital domains — including web-based attacks, dark web activities, and email*

	crimes — while maintaining integrity and admissibility of evidence. • *Prepare and present professional forensic findings by creating clear, structured reports and oral presentations that effectively communicate results and interpretations to both technical and non-technical audiences.*
Content	• *Computer Forensics Fundamentals* • *Computer Forensics Investigation Process* • *Understanding Hard Disks and File Systems* • *Data Acquisition and Duplication* • *Defeating Anti-forensics Techniques* • *Windows Forensics* • *Linux and Mac Forensics* • *Network Forensics* • *Investigating Web Attacks* • *Dark Web Forensics* • *Investigating Email Crimes* • *Malware Forensics*
Examination forms	***Exam*** ***Weight*** ***Date*** *Final* *25%* *TBA (to be announced)* *Quiz* *20%* *every 3 week* *Project* *25%* *TBA (to be announced)* *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 (25%)+Before Exam score will remain the same (75%)*
Reading list	*[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).*

Module designation	***CS 207 - Methodology of Scientific Research***
Semester(s) in which the module is taught	*Year 2, fall semester*
Person responsible for the module	*PhD.Tapdig Dunyamali* *BHOS White City Building ROOM 301* *tapdig.dunyamali@bhos.edu.az* *99412 5210000 ext. 33030*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Lectures, seminar, presentation, midterm, class test*
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, self-study = 10 h/ week*
Credit points	*6 ECTS*
Required and recommended prerequisites for joining the module	• *Basic academic writing skills* • *Foundations of the student's domain (e.g., cybersecurity, computer science)* • *Basic statistics and data analysis* • *Critical thinking and logical reasoning* • *Familiarity with scientific literature* • *Basic computer skills (word processing, spreadsheets, presentations)*
Module objectives/intended learning outcomes	• *Learn how to choose a research topic and formulate a proposal grounded in the programme's scientific domains; define clear research questions and objectives.* • *Develop a thorough understanding of quantitative and qualitative research methodologies and their applications; justify method selection with evidence.* • *Acquire practical skills in designing, conducting and analysing scientific studies, including hypothesis testing, sampling, instrumentation and data validation, with **reproducible** workflows and proper documentation.* • *Enhance critical thinking and analytical abilities for **systematic literature review**, source evaluation and synthesis; manage citations and research data responsibly.* • *Ensure proficiency in **research ethics**, integrity and legal compliance (consent, data protection, IRB-style approvals, plagiarism avoidance, open-science practices).* • *Apply learned methodologies to real-world cybersecurity problems; select appropriate models and evidence under uncertainty and argue risk/limitations.* • *Engage in hands-on mini-projects involving study design, data collection/analysis and reporting; deliver peer-reviewed drafts and revisions.*

	• *Improve scientific communication skills through well-structured written reports and oral presentations for specialist and non-specialist audiences; defend choices during Q&A.*
Content	• *Introduction to Research Methodology* • *Formulating Research Questions* • *Topic Selection, Literature Review, and Background Research* • *Developing Hypotheses* • *Designing Experiments* • *Data Collection Methods* • *Deep Dive into Data Analysis* • *Midterm Exam* • *Drawing Conclusions* • *Communicating Research Findings* • *Research Ethics and Integrity* • *Peer Review and Feedback*
Examination forms	***Exam*** ***Weight*** ***Date*** *Final* *35%* *TBA (to be announced)* *Midterm* *30%* *6th week of the semester* *Class tests* *10%* *every week* *Presentation* *25%* *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 (35%) +Before Exam score will remain the same (65%)*
Reading list	1. *Research Methodology, the aims, practices and ethics of science, by Peter Pruzan, 2016, International Publishing* 2. *Additional sources will be presented and shared by instructor during the semester*

Module designation	***CS 202 - Scientific Research Internship***
Semester(s) in which the module is taught	*Year 2, spring semester*
Person responsible for the module	*Assoc.Prof. Naila Allahverdiyeva* *BHOS White City Building ROOM 301* *naila.allahverdiyeva@bhos.edu.az* *99412 5210000 ext. 33030*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*Independent research, report writing, presentation, seminar discussion, supervision meetings*
Workload (incl. contact hours, self-study hours)	*Private study hours per week 15 hours*
Credit points	*6 ECTS*
Required and recommended prerequisites for joining the module	• *Basic academic writing and referencing skills* • *Familiarity with research methodology and data collection methods* • *Knowledge of core cybersecurity and computer science principles* • *Understanding of scientific ethics and plagiarism policies* • *Experience with documentation and presentation tools (Word, PowerPoint, Excel)*
Module objectives/intended learning outcomes	*• Apply theoretical and practical knowledge gained from the MSc program to an independent or supervised research project.* *• Demonstrate the ability to conduct problem-oriented, methodologically sound scientific investigation.* *• Formulate clear research objectives, hypotheses, and methodologies aligned with academic standards.* *• Collect, analyze, and interpret data relevant to a cybersecurity or information systems topic.* *• Prepare a professional-level research report that adheres to institutional and ethical requirements.* *• Present research findings effectively to both academic and non-academic audiences.* *• Collaborate with supervisors and research teams while managing time, resources, and reporting responsibilities.* *• Reflect on research outcomes to identify future work or publication opportunities.*
Content	• *Research topic selection and proposal development* • *Methodology planning and data collection techniques* • *Implementation and experimental work* • *Data analysis and interpretation* • *Documentation and report preparation* • *Research ethics, plagiarism prevention, and academic integrity* • *Interim reporting and supervisor feedback sessions* • *Final presentation and defense of research outcomes*

Examination forms	***Component*** — ***Weight*** *Performance Evaluation by Supervisor* — *50%* *Internship Report* — *50%*
Study and examination requirements	***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.*
Reading list	*Before starting the internship:* • *Internship Notice and Program* • *Individual Task Sheet* • *Thematic Task assigned by BHOS Department* *After completion:* • *Daily Logbook* • *Final Internship Report*

Module designation	***CS 204 - Pedagogical Internship***
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	*Compulsory*
Teaching methods	*Mentored teaching practice, observation, class delivery, laboratory supervision, feedback discussions, report writing*
Workload (incl. contact hours, self-study hours)	*Private study hours per week 15 hours*
Credit points	*6 ECTS*
Required and recommended prerequisites for joining the module	• *Successful completion of prior theoretical and laboratory-based modules in the MSc Cybersecurity curriculum* • *Competence in cybersecurity domains (network defense, digital forensics, risk management, and cloud security)* • *Completion of the Methodology of Scientific Research module* • *Basic pedagogical knowledge or willingness to engage in reflective teaching practice*
Module objectives/intended learning outcomes	• *Apply academic knowledge from cybersecurity courses in a teaching or mentoring environment, demonstrating the ability to plan and deliver effective learning sessions.* • *Develop teaching, communication, and mentoring skills by conducting seminars, laboratory demonstrations, and student consultations under faculty supervision.* • *Design instructional materials (lectures, labs, or tutorials) that integrate cybersecurity concepts with practical examples and ethical considerations.* • *Assess and evaluate student performance, providing constructive feedback aligned with academic learning outcomes.* • *Demonstrate classroom management, professional ethics, and adherence to institutional teaching standards.* • *Reflect critically on teaching experiences and identify areas for professional growth.* • *Communicate technical cybersecurity topics clearly to diverse audiences, adjusting the level of complexity appropriately.*

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

- *Introduction to pedagogy in higher education*
- *Lesson planning and learning-outcome mapping*
- *Teaching observation and feedback cycles*
- *Laboratory supervision and mentoring practices*
- *Assessment design and evaluation strategies*
- *Professional conduct and ethical behavior in academic settings*
- *Reflective journaling and peer feedback*
- *Final teaching demonstration and report submission*

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

Assessment Type	**Weight**
Pedagogical report	50 %
Teaching demonstration / Observation	30 %
Supervisor evaluation	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 will be graded out of 90%, and 10% for quiz will remain unchanged.</td></tr>
<tr><td>Reading list</td><td>

1. *L. S. Vygotsky, Mind in Society: The Development of Higher Psychological Processes, Harvard University Press, 1978.*
2. *D. Kolb, Experiential Learning: Experience as the Source of Learning and Development, Pearson, 2015.*
3. *James H. Stronge, Qualities of Effective Teachers, ASCD, 2018.*
4. *John Biggs & Catherine Tang, Teaching for Quality Learning at University, Open University Press, 2011.*
5. *Recent institutional and IEEE/ACM cybersecurity education frameworks and pedagogical standards.*

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

Module designation	***CS 206 - Master Thesis***
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	*Compulsory*
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)	*Private study hours per week 45 hours*
Credit points	*18 ECTS*
Required and recommended prerequisites for joining the module	• *Completion of all core Cybersecurity 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	• *Identify a significant and research-worthy problem within the cybersecurity domain and formulate a clear research question and objectives.* • *Conduct a comprehensive literature review, critically evaluating existing works and identifying gaps, challenges, and opportunities.* • *Apply suitable **research methodologies** (quantitative, qualitative, experimental, or hybrid) for collecting, analysing, and interpreting data.* • *Design and implement **experiments, models, or prototypes** relevant to cybersecurity issues, applying technical and analytical reasoning.* • *Demonstrate **independent problem-solving skills**, scientific integrity, and adherence to ethical standards in research.* • *Analyse results, interpret findings, and provide evidence-based conclusions supported by data, experiments, or simulations.* • *Write a well-structured academic thesis consistent with scientific and institutional formatting standards.* • ***Defend research findings** effectively during the oral examination, demonstrating professional communication skills and critical reflection.* • *Evaluate limitations, societal implications, and potential future directions of the conducted research.*

Content	• *Selection and approval of a cybersecurity-related research topic* • *Formulation of research questions, hypotheses, and objectives* • *Comprehensive literature review and gap analysis* • *Research design and methodology development* • *Data collection, experiment setup, or system implementation* • *Statistical analysis, validation, and result interpretation* • *Thesis structure, documentation, and writing process* • *Defense preparation, presentation, and response to examiner questions* • *Ethical and academic integrity in research*
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	***CS 112 - Developing safe distributed systems***
Semester(s) in which the module is taught	*Year 1, spring semester*
Person responsible for the module	*Khayyam Masiyev* *BHOS White City Building ROOM 301* *Khayyam.masiyev@bhos.edu.az* *99412 5210000 ext. 33030*
Language	*English*
Relation to curriculum	*Elective*
Teaching methods	*Lectures, laboratory, presentation, project*
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, self-study = 8.5 h/ week*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	• *Fundamentals of Distributed Systems* • *Network Security* • *Operating Systems* • *Programming in Java, Python, or Go*
Module objectives/intended learning outcomes	• *Demonstrate understanding of distributed system architectures, including client-server, peer-to-peer, and microservices models.* • *Analyze security challenges specific to distributed systems, including data integrity, confidentiality, and availability.* • *Design and implement secure communication protocols, including TLS, end-to-end encryption, and secure RPC.* • *Apply consensus algorithms and cryptographic techniques to ensure system reliability and security.* • *Detect, prevent, and respond to security attacks in distributed applications.* • *Evaluate distributed systems using modern security testing tools and techniques.* • *Integrate security best practices into cloud-based and blockchain-based distributed systems.*
Content	• *Introduction to Distributed Systems – Overview, key concepts, advantages, challenges* • *Distributed System Architectures – Client-server, peer-to-peer, microservices, hybrid architectures* • *Security Principles in Distributed Systems – CIA triad, threat modeling, risk assessment* • *Secure Communication Protocols – TLS/SSL, SSH, VPNs, end-to-end encryption*

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

- *Authentication and Authorization – Identity management, OAuth, Kerberos, RBAC, access control models*
- *Consensus Algorithms – Paxos, Raft, Byzantine Fault Tolerance, blockchain consensus*
- *Fault Tolerance and Resilience – Replication, redundancy, recovery, high availability*
- *Security Threats and Attack Vectors – DoS/DDoS, Man-in-the-Middle, replay attacks, insider threats, supply chain attacks*
- *Secure Coding for Distributed Systems – Input validation, secure API design, sandboxing, preventing vulnerabilities*
- *Cloud Security and Microservices – Container security (Docker/Kubernetes), secure deployment in cloud*
- *Monitoring, Logging, and Intrusion Detection – Security monitoring, auditing, log analysis, anomaly detection, incident response*

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

Exam	***Weight***	***Date***
Final	*40%*	*TBA (to be announced)*
Project	*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>

[1] Coulouris, G., Dollimore, J., Kindberg, T., & Blair, G. – Distributed Systems: Concepts and Design, 5th Edition.

[2] Shapiro, M. – Designing Secure Distributed Systems, O'Reilly, 2020.

[3] Tanenbaum, A., & Van Steen, M. – Distributed Systems: Principles and Paradigms, 3rd Edition.

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

Module designation	***CS 114 - Cybersecurity Operations and Defense***
Semester(s) in which the module is taught	*Year 1, spring semester*
Person responsible for the module	*Nihad Alili* *BHOS White City Building ROOM 301* *nihad.elili@bhos.edu.az* *99412 5210000 ext. 33030*
Language	*English*
Relation to curriculum	*Elective*
Teaching methods	*Lectures, laboratory, presentation, project*
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, self-study = 8.5 h/ week*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	• *Networking fundamentals (TCP/IP, routing, switching)* • *Operating systems (Windows, Linux)* • *Basic cybersecurity concepts (CIA triad, malware, firewalls, IDS/IPS)* • *Understanding of cryptography principles and authentication mechanisms*
Module objectives/intended learning outcomes	• *Demonstrate knowledge of cybersecurity operations and defense strategies in enterprise environments.* • *Monitor networks and systems using modern security tools and platforms.* • *Identify, analyze, and respond to cyber threats and incidents.* • *Implement preventive and detective controls to secure IT infrastructure.* • *Apply incident response and digital forensics techniques to mitigate attacks.* • *Design and manage security policies, procedures, and operational plans.* • *Evaluate emerging threats and develop strategic defense solutions.*
Content	• ***Introduction to Cybersecurity Operations*** *– SOC overview, cyber defense strategies* • ***Threat Landscape and Attack Vectors*** *– Malware, phishing, APTs, insider threats* • ***Network Defense Fundamentals*** *– Firewalls, IDS/IPS, segmentation, honeypots* • ***Endpoint Security and Hardening*** *– Anti-malware, OS hardening, host monitoring* • ***Security Monitoring and SIEM*** *– Log collection, analysis, alerts*

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

Vulnerability Management and Patch Operations – Scanning, patching, risk assessment
Incident Response Planning – IR frameworks, plan creation, tabletop exercises
Digital Forensics Basics – Evidence collection, forensic imaging, chain of custody
Malware Analysis and Threat Hunting – Static/dynamic analysis, threat hunting methodology
Cloud and Application Security Operations – Cloud monitoring, container security
Security Automation and Orchestration – SOAR, automation scripts, defensive responses

</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>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>

William Stallings, Network Security Essentials: Applications and Standards, 7th Edition.
Michael E. Whitman, Herbert J. Mattord, Principles of Incident Response and Disaster Recovery, 3rd Edition.
Mark Ciampa, Security+ Guide to Network Security Fundamentals, 7th Edition.

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

Module designation	***CS 116 - Stenography***
Semester(s) in which the module is taught	*Year 1, spring semester*
Person responsible for the module	*Agha Aghayev* *BHOS White City Building ROOM 301* *aga.agayev@bhos.edu.az* *99412 5210000 ext. 33030*
Language	*English*
Relation to curriculum	*Elective*
Teaching methods	*Lectures, laboratory, presentation, project*
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, self-study = 8.5 h/ week*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	• *Fundamentals of cybersecurity* • *Computer networks and protocols* • *Cryptography basics* • *Programming skills (Python, C/C++, or Java)* • *Digital media basics (images, audio, video)*
Module objectives/intended learning outcomes	• *Explain the principles and history of steganography.* • *Implement steganography algorithms for images, audio, and video.* • *Conduct steganalysis to detect hidden information.* • *Analyze and compare the security and efficiency of different steganography techniques.* • *Apply steganography in secure communication and forensic investigations*
Content	• *Introduction to Steganography – History, principles, and applications* • *Classical Steganography – Text and linguistic methods* • *Image Steganography Basics – LSB embedding* • *Advanced Image Steganography – Transform domain techniques (DCT, DWT)* • *Audio Steganography Basics – LSB and phase coding* • *Advanced Audio & Video Steganography – Spread spectrum, echo hiding* • *Network Steganography – Covert channels and protocol hiding* • *Steganalysis Introduction – Detect hidden messages in media* • *Advanced Steganalysis – Statistical and machine learning methods* • *Steganography in Cybersecurity – Secure communications and messaging*

Examination forms	***Exam***	***Weight***	***Date***
	Final	*40%*	*TBA (to be announced)*
	Project	*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] Jessica Fridrich, Steganography in Digital Media: Principles, Algorithms, and Applications, Cambridge University Press, 2009.* *[2] Neil F. Johnson, Zoran Duric, Sushil Jajodia, Information Hiding: Steganography and Watermarking – Attacks and Countermeasures, Springer, 2001.* *[3] Stefan Katzenbeisser, Fabien A. P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, 2000.*		

Module designation	***CS 118 - Biometric Systems Security***
Semester(s) in which the module is taught	*Year 1, spring semester*
Person responsible for the module	*Gunay Abdiyeva Aliyeva* *BHOS White City Building ROOM 301* *gunay.abdiyeva@bhos.edu.az* *99412 5210000 ext. 33030*
Language	*English*
Relation to curriculum	*Elective*
Teaching methods	*Lectures, laboratory, presentation, project*
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, self-study = 8.5 h/ week*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	• *Cybersecurity fundamentals* • *Computer networks basics* • *Cryptography essentials* • *Operating systems knowledge* • *Programming/scripting skills* • *Mathematics and statistics* • *Basic digital signal/image processing* • *Ethical and legal awareness in cybersecurity*
Module objectives/intended learning outcomes	• *Understand fundamental biometric concepts and modalities (fingerprint, iris, face, voice, gait, etc.).* • *Analyze biometric system architectures and components.* • *Identify and evaluate vulnerabilities and attacks on biometric systems.* • *Apply methods for secure design, implementation, and deployment of biometric systems.* • *Understand privacy, legal, and ethical issues in biometric security.* • *Implement biometric security measures for practical applications*
Content	• *Introduction to biometrics: types, applications, and security importance* • *Biometric modalities: fingerprint, face, iris, voice, behavioral* • *Biometric system architecture: sensors, feature extraction, matching* • *Biometric data representation: templates, feature vectors, storage* • *Biometric authentication: verification vs. identification, performance metrics* • *Biometric attacks: spoofing, replay, template attacks*

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

- *Anti-spoofing and liveness detection techniques*
- *Cryptographic protection of biometric data: encryption, hashing, secure storage*
- *Multimodal biometrics and fusion techniques*
- *Privacy, legal, and ethical considerations*
- *Emerging trends: behavioral biometrics, AI in biometrics, mobile biometrics*

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

Exam	***Weight***	***Date***
Final	*40%*	*TBA (to be announced)*
Project	*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>

1. *Jain, A.K., Ross, A., & Nandakumar, K. Introduction to Biometrics, Springer, 2011.*
2. *Li, S.Z. & Jain, A.K. Encyclopedia of Biometrics, Springer, 2015.*
3. *Ratha, N.K., Connell, J.H., & Bolle, R.M. Enhancing Security and Privacy in Biometrics, Springer, 2007.*
4. *Selected research papers, journal articles, and online resources*

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

Module designation	***CS 209 - Malware Analysis***
Semester(s) in which the module is taught	*Year 2, spring semester*
Person responsible for the module	*Nihad Alili* *BHOS White City Building ROOM 301* *nihad.elili@bhos.edu.az* *99412 5210000 ext. 33030*
Language	*English*
Relation to curriculum	*Elective*
Teaching methods	*Lectures, laboratory, presentation, project*
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)* *Laboratory: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, self-study = 10 h/ week*
Credit points	*6 ECTS*
Required and recommended prerequisites for joining the module	• *Fundamentals of cybersecurity and network security* • *Basic programming skills (Python, C/C++)* • *Operating systems concepts (Windows, Linux)* • *Basic knowledge of computer forensics*
Module objectives/intended learning outcomes	• *Identify different types of malware and understand their behavior.* • *Apply static and dynamic malware analysis techniques.* • *Utilize reverse engineering tools to dissect malicious software.* • *Understand malware propagation methods and infection vectors.* • *Evaluate malware using sandboxing and automated analysis tools.* • *Develop strategies to mitigate malware threats and protect systems.* • *Conduct real-world malware investigations in a controlled environment.*
Content	• *Introduction to malware: types, motives, and threats* • *Malware propagation techniques: viruses, worms, trojans, ransomware* • *Static analysis: file inspection, disassembly, signature identification* • *Dynamic analysis: sandboxing, behavior monitoring, network analysis* • *Reverse engineering malware: debugging, decompiling, unpacking* • *Memory analysis and forensic techniques* • *Malware detection evasion techniques* • *Automated malware analysis tools and platforms* • *Rootkits and bootkits analysis*

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

- *Network-based malware analysis*
- *Malware mitigation strategies and response planning*

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

Exam	***Weight***	***Date***
Final	*40%*	*TBA (to be announced)*
Project	*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>

[1] Michael Sikorski, Andrew Honig – Practical Malware Analysis, 2nd Edition, 2012
[2] Monnappa K A – Malware Analyst's Cookbook and DVD, 2010

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

Module designation	***CS 112 - Development, Security, and Operations (DevSecOps)***
Semester(s) in which the module is taught	*Year 2, spring semester*
Person responsible for the module	*Lecturer Elshan Farzaliyev* *BHOS White City Building ROOM 301* *elshan.farzaliyev@bhos.edu.az* *99412 5210000 ext. 33030*
Language	*English*
Relation to curriculum	*Elective*
Teaching methods	*Lectures, laboratory, presentation, project*
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)* *Laboratory: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, self-study = 10 h/ week*
Credit points	*6 ECTS*
Required and recommended prerequisites for joining the module	• *Fundamentals of cybersecurity and network security* • *Basic software development knowledge (programming in Python, Java, or C/C++)* • *Familiarity with operating systems (Windows, Linux)* • *Understanding of cloud computing concepts* • *Knowledge of version control systems (e.g., Git)*
Module objectives/intended learning outcomes	• *Explain the principles and practices of DevSecOps.* • *Integrate security into the software development lifecycle (SDLC).* • *Implement CI/CD pipelines with automated security checks.* • *Apply vulnerability scanning and secure code analysis tools.* • *Manage configuration, compliance, and secrets securely in development environments.* • *Monitor applications and infrastructure for security incidents.* • *Develop strategies for incident response and mitigation in DevSecOps workflows.*
Content	• *Introduction to DevSecOps: concepts, culture, and benefits* • *Secure software development lifecycle (SDLC) integration* • *Continuous Integration / Continuous Deployment (CI/CD) pipelines* • *Automated security testing: SAST, DAST, dependency scanning* • *Container security and orchestration (Docker, Kubernetes)* • *Infrastructure as Code (IaC) security* • *Secrets management and configuration security* • *Cloud security and DevSecOps in cloud environments* • *Monitoring, logging, and incident detection* • *Threat modeling and vulnerability management in DevSecOps* • *Compliance, audit, and security metrics*

Examination forms	***Exam***	***Weight***	***Date***
	Final	*40%*	*TBA (to be announced)*
	Project	*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	• *Jim Bird – DevSecOps: A leader's guide to producing secure software without compromising flow, feedback, and continuous improvement, 2020* • *Nicole Forsgren, Jez Humble, Gene Kim – Accelerate: The Science of Lean Software and DevOps, 2018*		

Module designation	***CS 213 - Systems Engineering Processes***
Semester(s) in which the module is taught	*Year 2, spring semester*
Person responsible for the module	*Lecturer Khayyam Masiyev* *BHOS White City Building ROOM 301* *khayyam.masiyev@bhos.edu.az* *99412 5210000 ext. 33030*
Language	*English*
Relation to curriculum	*Elective*
Teaching methods	*Lectures, laboratory, presentation, project*
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)* *Laboratory: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, self-study = 10 h/ week*
Credit points	*6 ECTS*
Required and recommended prerequisites for joining the module	• *Fundamentals of cybersecurity and information systems* • *Basic knowledge of software and hardware systems* • *Understanding of networking principles and protocols* • *Familiarity with project management concepts* • *Basic knowledge of system modeling tools (optional)*
Module objectives/intended learning outcomes	• *Explain systems engineering concepts and lifecycle processes.* • *Develop and analyze system requirements for secure systems.* • *Apply system design methodologies including modeling and simulation.* • *Integrate security considerations into system architecture and design.* • *Conduct risk assessment, reliability analysis, and trade-off studies.* • *Perform system verification, validation, and testing.* • *Manage systems engineering projects with iterative and agile approaches.*
Content	• *Introduction to Systems Engineering and Processes* • *Systems lifecycle models: Waterfall, V-model, Spiral, Agile* • *Requirements engineering and management* • *System architecture and design principles* • *Security integration in system design* • *Risk management and reliability analysis* • *Modeling and simulation of complex systems* • *Verification and validation techniques* • *Testing strategies for cybersecurity systems* • *System integration and deployment* • *Systems maintenance, evolution, and sustainability*
Examination forms	***Exam*** ***Weight*** ***Date***

	Final	*40%*	*TBA (to be announced)*
	Project	*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	• *Blanchard, B.S., & Fabrycky, W.J. – Systems Engineering and Analysis, 5th Edition, 2010* • *INCOSE – Systems Engineering Handbook, 4th Edition, 2015*		

Module designation	***CS 215 - Advanced Database Systems***
Semester(s) in which the module is taught	*Year 2, spring semester*
Person responsible for the module	*Assoc. Prof.Mahammad Sharifov* *BHOS White City Building ROOM 301* *mahammad.sharifov@bhos.edu.az* *99412 5210000 ext. 33030*
Language	*English*
Relation to curriculum	*Elective*
Teaching methods	*Lectures, laboratory, presentation, project*
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)* *Laboratory: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, self-study = 10 h/ week*
Credit points	*6 ECTS*
Required and recommended prerequisites for joining the module	• *Basic database concepts (SQL, relational databases)* • *Fundamentals of cybersecurity* • *Understanding of data structures and algorithms* • *Knowledge of operating systems and networking basics*
Module objectives/intended learning outcomes	• *Analyze advanced database architectures (distributed, NoSQL, NewSQL).* • *Apply techniques for database optimization, indexing, and query performance tuning.* • *Implement security measures for database systems, including access control, encryption, and auditing.* • *Manage transactions, concurrency, and recovery in secure environments.* • *Integrate database systems with cybersecurity solutions and applications.* • *Evaluate emerging database technologies and trends from a security perspective.* • *Design, implement, and maintain secure database systems for real-world applications.*
Content	• *Advanced relational database design and normalization* • *Query optimization and performance tuning* • *Indexing techniques and materialized views* • *Distributed databases and replication strategies* • *NoSQL databases: key-value, document, column-family, graph* • *Transaction management and concurrency control* • *Backup, recovery, and fault tolerance* • *Database security principles: authentication, authorization, and encryption* • *SQL injection and other database attack mitigation* • *Auditing, monitoring, and compliance in databases*

	• *Emerging trends: cloud databases, blockchain-based storage, and NewSQL systems*
Examination forms	***Exam*** ***Weight*** ***Date*** *Final* *40%* *TBA (to be announced)* *Project* *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] Silberschatz, A., Korth, H., & Sudarshan, S. – Database System Concepts, 7th Edition, 2019* *[2] Elmasri, R., & Navathe, S. – Fundamentals of Database Systems, 7th Edition, 2015* *[3] Coronel, C., & Morris, S. – Database Systems: Design, Implementation, & Management, 13th Edition, 2020*

Module designation	***CS 217 - Reverse Engineering***
Semester(s) in which the module is taught	*Year 2, spring semester*
Person responsible for the module	*Nihad Alili* *BHOS White City Building ROOM 301* *nihad.elili@bhos.edu.az* *99412 5210000 ext. 33030*
Language	*English*
Relation to curriculum	*Elective*
Teaching methods	*Lectures, laboratory, presentation, project*
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)* *Laboratory: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, self-study = 10 h/ week*
Credit points	*6 ECTS*
Required and recommended prerequisites for joining the module	• *Programming in C/C++ and Python* • *Basic understanding of computer architecture and operating systems* • *Assembly language fundamentals* • *Familiarity with cybersecurity concepts and malware analysis*
Module objectives/intended learning outcomes	• *Understand the principles and goals of reverse engineering.* • *Analyze binary executables to determine software behavior.* • *Disassemble and interpret assembly code for x86/x64 architectures.* • *Use debugging and reverse engineering tools (e.g., IDA Pro, Ghidra, OllyDbg).* • *Identify software vulnerabilities and understand their exploitation potential.* • *Reverse engineer malware to detect malicious behaviors and extract indicators of compromise.* • *Apply safe reverse engineering practices in controlled lab environments.* • *Produce detailed technical reports documenting reverse engineering findings.*
Content	• *Introduction to Reverse Engineering: objectives, ethics, and legal considerations* • *Software compilation, linking, and executable formats* • *Introduction to assembly language and machine code* • *Static analysis of binaries: disassemblers and decompilers* • *Dynamic analysis and debugging techniques* • *Reverse engineering of Windows and Linux executables* • *Malware reverse engineering and behavioral analysis* • *Packing, obfuscation, and anti-reverse engineering techniques* • *Binary exploitation and vulnerability discovery*

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

- *Scripting for automation in reverse engineering*
- *Reporting and documentation of reverse engineering results*

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

Exam	***Weight***	***Date***
Final	*40%*	*TBA (to be announced)*
Project	*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>

[1] Eilam, E. – Reversing: Secrets of Reverse Engineering, 2nd Edition, 2011

[2] Sikorski, M., & Honig, A. – Practical Malware Analysis, 2nd Edition, 2012

[3] Dang, J., et al. – IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler, 2nd Edition, 2011

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

Module designation	***CS 219 - Advanced Cloud Computing***
Semester(s) in which the module is taught	*Year 2, spring semester*
Person responsible for the module	*Nihad Alili* *BHOS White City Building ROOM 301* *nihad.elili@bhos.edu.az* *99412 5210000 ext. 33030*
Language	*English*
Relation to curriculum	*Elective*
Teaching methods	*Lectures, laboratory, presentation, project*
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)* *Laboratory: 24 h (2 h / week)* ***Contact hours:*** *Examination preparation, consultation, self-study = 10 h/ week*
Credit points	*6 ECTS*
Required and recommended prerequisites for joining the module	• *Basic cloud computing concepts (IaaS, PaaS, SaaS)* • *Networking fundamentals and virtualization* • *Operating system and Linux administration* • *Cybersecurity principles*
Module objectives/intended learning outcomes	• *Understand cloud computing models and architectures, including public, private, hybrid, and multi-cloud.* • *Evaluate cloud service providers and deployment models for security considerations.* • *Implement and secure virtualization and containerization environments.* • *Analyze cloud-specific threats and vulnerabilities.* • *Apply identity and access management (IAM) and encryption in cloud environments.* • *Deploy secure cloud applications and monitor for threats.* • *Understand compliance, governance, and regulatory requirements in cloud computing.* • *Perform cloud security assessments and recommend mitigation strategies.*
Content	• *Introduction to advanced cloud computing and service models* • *Cloud architectures: public, private, hybrid, multi-cloud* • *Virtualization security and hypervisors* • *Containerization and orchestration (Docker, Kubernetes)* • *Cloud storage security and data protection* • *Identity and access management in the cloud* • *Cloud network security and monitoring* • *Threats and vulnerabilities in cloud environments* • *Cloud compliance, governance, and regulatory frameworks* • *Cloud incident response and disaster recovery* • *Security assessment of cloud systems*

Examination forms	***Exam***	***Weight***	***Date***
	Final	*40%*	*TBA (to be announced)*
	Project	*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] Buyya, R., Vecchiola, C., & Selvi, S. T. – Mastering Cloud Computing, 2nd Edition, 2013* *[2] Jamsa, K. – Cloud Computing: SaaS, PaaS, IaaS, Virtualization, Business Models, Mobile, Security and More, 2013* *[3] Zissis, D., & Lekkas, D. – Securing Cloud Services, 2012*		