**The Ministry of Education of the Azerbaijan Republic**

**The State Oil Company of the Azerbaijan Republic**

**Baku Higher Oil School**

“Approved by”

Rector of Baku Higher Oil School

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Elmar Gasimov**

“\_\_\_\_”\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2023-ci il

Process Automation Engineering Department

Information Security Division

Systems Analysis and Design

**Courses Syllabus**

Spring, 2023

Instructor : Khayyam H. MASIYEV

Course code: Course credit : 5

Office : Campus Aypara Office hours : M-F 09.00-16.00

Prerequisites: ICT 1 & 2

Language of instruction: English

Schedule :

QR. IS-19.1: Lecture, Laboratory, Seminar Tuesday & Thursday

Web site :

Email : [khayyam.masiyev@bhos.edu.az](mailto:khayyam.masiyev@bhos.edu.az)

**Description about course**

This course explores the methodologies and theories involved in system design. Class lecture and assignments revolve around a case study analysis used to illustrate the basic concepts, methodologies and techniques used in the design of computerized systems.

Each of the phases of the Systems Development Life Cycle: (Planning, Analysis, Design, Implementation, and Support) are covered in this case study.

In a Systems Analysis and Design course with a focus on information security, individual/group semester projects involve applying principles and methodologies of systems analysis and design to address real-world security challenges.

These projects aim to enhance students' understanding of information security by having them analyze security-related case studies (projects, scenarios) and develop solutions or system designs that mitigate security risks.

**Define**: An information security individual/group semester project in a Systems Analysis and Design course is an academic endeavor where students choose a real-world case study (projects, scenarios) related to information security issues or breaches.

They then apply their knowledge of systems analysis and design to develop solutions, designs, or strategies that address the security weaknesses identified in the chosen case study/project. (They then apply principles of systems analysis and design to propose solutions, enhancements, or strategies aimed at addressing these security issues.)

These projects typically involve defining system requirements, conducting security assessments, and proposing improvements to ensure the confidentiality, integrity, and availability of data and systems.

The primary goal is to gain theoretical and practical experience in solving real-world security problems through systematic analysis and design methodologies.

**Semester Projects**: Students undertaking these projects will follow a structured approach that includes:

1. **Case Study/ Scenario Selection**: In this project, students select (from the below list) real-world projects or scenarios related to information security. These scenarios can be drawn from actual organizations, businesses, or projects, where information security issues or improvements are needed. (Choose a real-world case study, typically involving a security incident, data breach, or security-related challenge. The case study serves as the foundation for the project.)
2. **Analysis:** Students begin by conducting a thorough analysis of the selected real-world projects. They aim to identify the root causes, security weaknesses, vulnerabilities, or compliance gaps that need to be addressed. (Analyze the case study thoroughly, identifying the security vulnerabilities, weaknesses, or compliance issues that led to the incident or challenge. Understand the context and consequences of the incident.)
3. **Requirements Gathering:** Define specific security requirements based on the analysis. Determine what needs to be addressed to prevent similar security issues in the future. (Based on their analysis, students define information security requirements. These requirements outline what changes, enhancements, or measures are necessary to mitigate the identified security risks within the context of the real-world projects.)
4. **System Design:** Apply systems analysis and design principles to create a detailed system design that addresses the identified security requirements. (Applying systems analysis and design methodologies, students create a detailed system design that addresses the identified security requirements.) This may include architectural diagrams, data flow diagrams, system components and all other UML diagrams (which we will learn and discuss in a duration of SAD course).
5. **Security Enhancements:** Develop and propose security enhancements, solutions, or strategies to mitigate the vulnerabilities identified in the project. (Students then develop and propose security enhancements, solutions, or strategies tailored to the real-world projects.) These enhancements may encompass technical, procedural, or organizational changes to improve information security.
6. **Documentation:** Create comprehensive project documentation report (Students prepare Technical Specification Report), which includes system requirements, design specifications, security policies, and implementation plans, all aligned with the real-world projects.
7. **Presentation:** Present the project to the class / instructor, explaining the case study, the analysis conducted, and the proposed solutions. (Finally, students present their project findings and proposed solutions to their peers and instructors. This presentation helps them effectively communicate their analysis, design, and recommendations in the context of the real-world projects.)

**Course objective section**

This course introduces established and evolving methodologies for the analysis, design, and development of an information system.

**Benefits and Learning outcomes section**

Emphasis is placed on system characteristics, managing projects, prototyping, CASE/OOM tools, and systems development life cycle phases.

Upon completion, students should be able to analyze a problem and design an appropriate solution using a combination of tools and techniques.

1. **Practical Experience:** Students gain practical experience in analyzing real-world security challenges and proposing solutions, preparing them for real-world scenarios.
2. **Application of Concepts:** They apply systems analysis and design concepts and methodologies learned in the course to address specific information security concerns in a real-world context.
3. **Critical Thinking:** Students develop critical thinking skills by assessing and mitigating security vulnerabilities within the context of the chosen real-world samples. (Students develop critical thinking skills as they assess and mitigate security vulnerabilities within the real-world projects, considering the unique challenges they present.)
4. **Communication Skills:** The semester project encourages effective communication as students must convey their analysis and solutions clearly to their peers and instructors.

**Assessment methods**

The exams (HWs/Case Studies + Semester Final Project) are done using exam papers and pen. Parts of Quiz & Final exams are consisting with test questions & classic questions (written examination). All questions must be answered.

**Grading (NEW)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Exam** | **Weight** | **Date** | **Exam minutes** |
| *HWs/Case Studies* or *Product* (Development, Cloud integration, Testing) | 30 % | after each course chapter | Deadline (to be announced end of each course chapter) |
| Individual / Group Seminar (Individual Research Report) | 70 % | last lecture week | 20 min. for each project (including PowerPoint, Project  presentation + Research Report)  Note: Students needs to upload semester project resources (as .zip) to the LMS till deadline (11th of the week) |

**NOTE :**

1. **Total number of hws/labs are 10-11 course chapters (groups of hws/case studies in each course chapter). Each hw/case study is graded separately. Student needs to bring (upload each home work as a document file to the LMS system) their hws/case studies reports till deadline (which will be announced end of each course chapter). At the end of the term the average mark of the hws/labs are calculated.**
2. **Individual/Group Seminar Mark (Grade) = 50% Presentation + 50% Research report. Presentation and Research report needs to be send till deadline (will be announced in the class) upload each as a document file (Word and PowerPoint) to the LMS system.**
3. **Deadline is very important. In that case please send (upload to the LMS system) all your HWs/Labs and Seminar project till deadline. Otherwise your homeworks and seminar project will not be evaluated.**

**RESIT grading (**in case of fail Final exam**):**

Weight: **70%** Date: TBA (to be announced) Exam duration: 120 – 180 minutes

**Area grading scale**

A 91-100

B 81-90

C 71-80

D 61-70

F ≤ 60

**Rules**

**Exams**

In order to be excused from the exam, the student must contact the dean and the instructor before the exam. Excuse will not be granted for social activities such as trips, cruises and sporting events (unless you are participating). The exams will all be cumulative. Most of the questions on each exam will be taken from the chapters covered since the last exam.

But some will come from the earlier chapters. In general, the coverage will reflect the amount of the time spend in class on the different chapters.

**Withdrawal (pass / fail)**

This course strictly follows grading policy of the Process Automation Engineering Department (including Information Security Division). Thus, a 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 to pass Resit or required to repeat the course the following term or year in case of failed Resit.

**Late policy**

Late assignment (Individual Seminar) submissions won’t be accepted for grading. The grade for this assignment will be zero.

**Teaching resources**

Presentation : Systems Analysis and Design (in site: [www.lms.bhos.edu.az](http://www.lms.bhos.edu.az))

Textbook :

[1] Systems Analysis and Design, 12th edition, Scott Tilley, (2020)

[2] Agile Model-Based Systems Engineering Cookbook, Dr. Bruce Powel Douglass (2021)

[3] Modern Systems Analysis and Design, 9th edition, Joseph S. Valacich, Joey F. George (2021)

[4] Olga Filipova, Rui Vilão, “Software Development From A to Z”, Apress (2019)

[5] “Software Engineering, 10th Edition-Pearson, Ian Sommerville, (2020)

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 + instructor course recourses. All needed textbooks and resources will be announced by course instructor.

**Attendance**

The students are required to attend all classes as a part of their studies and those having legitimate reasons for absence (illness, family bereavement, etc.) are required to inform the instructor.

Quizzes date and time will not announce (inform) to students. In that case all students needs to attend all classes as a part of their studies.

**Professionalism and Participation**

1. Attend class regularly, arrive on time, leave only when dismissed

2. Attend class with all materials required, be prepared to listen and work

3. Be well prepared for class, read all required materials, and complete all necessary preparation

4. Be attentive in class, take notes, contribute to discussion and ask intelligent questions

5. Demonstrate professional and respectful interpersonal relationships with peers and instructor: ATTITUDE COUNTS, AND whining is unacceptable

6. Take responsibility for your actions, and your results

**Plagiarism**

Honesty requires that any ideas or material taken from another source for written, visual, or oral use must be fully acknowledged. Offering the work of someone else as one’s own is plagiarism. The language or ideas thus taken from another may range from isolated formulas, images, sentences or paragraphs to entire articles copied from books, periodicals, speeches, or the writings and creations of other students. The offering of materials assembled or collected by others in the form of projects or collections without acknowledgment also is considered plagiarism. Any student who fails to give credit for ideas or materials taken from another course is guilty of plagiarism.

|  |  |  |
| --- | --- | --- |
| **Week** | **Topics** | **Summary Description** |
| 1 | **Introduction to SAD. Course overview** | Week 1 provides an up to-date overview of IT issues, major trends, and various systems development approaches, including structured (traditional), object-oriented, and agile methods.  **Practice Day:**  Students needs to create group with 2-3 members. Students needs to choose semester project title. |
| 2 | **Systems Planning: The Systems Development Environment (Analysing the Business Case)**  (Introduction. Information Systems Projects. Evaluation of Systems Requests. Overview of and Evaluating Feasibility) | Week 2 offers a business-related starting point for successful systems analysis. Topics include strategic planning, review of systems requests, how to conduct a feasibility study, and the steps in a preliminary investigation. Topics include Evaluation of Systems Requests. Overview of and Evaluating Feasibility.  **Practice Day:**  Students needs to create group with 2-3 members. Students needs to choose semester project title. And discuss why they choose this project, and how they will start to work on this project. |
| 3 | **Systems Planning: Managing Systems Projects** (Introduction. Overview of Project Management.) | * explains project management, cost estimating, and change control for information systems. This chapter includes hands-on skills that systems analysts/engineers can use to create Gantt charts and PERT charts. * describe how to represent and schedule project plans using Gantt charts and network diagrams * explain how commercial project management software packages can be used to assist in representing and managing project schedules * Project Activities and Planning Steps. Create a Work Breakdown Structure. Identify Task Patterns. Calculate the Critical Path.   **Practice Day:**  Students projects discussion day. Students continue to work on their projects and preparing technical specification report. |
| 4 | **Agile System Programming vs Traditional System Programming** | Week 4 explains Agile programming concepts and techniques. This course also explains Scrum Master, Product Owner and Development Team concepts and techniques.  **Practice Day:**  Students projects discussion day. Students continue to work on their projects and preparing technical specification report. |
| 5 | **Systems Planning: Determining System Requirements - Requirements Modeling, Data and Process Modeling.**  **System Planning: Structuring System Process Requirements - Object Modeling, Development Strategies.** | * Week 5 describes fact-finding techniques and team-based modeling methods, including JAD and RAD, that systems analysts use to model and document a new system. * Week 5 also explains how systems analysts create a logical model for the new system by using data flow diagrams and process description tools, including structured English, decision tables, and decision trees. * Week 5 explains object-oriented tools and techniques, including use case diagrams, class diagrams, sequence diagrams, state-transition diagrams, activity diagrams, and the Unified Modeling Language. * Week 5 focuses on software acquisition options, including outsourcing and offshore outsourcing options, application service providers, and other trends that view software as a service rather than a product.   **Practice Day:**  Students projects discussion day. Requirements Engineering: students continue to work on their projects and on technical specification report. |
| 6 | **Systems Design**: System User Interface Design. System Data Design. | * Week 6 highlights output and report design, the interaction between humans and computers, including usability issues, graphical screen design, input issues, and data entry guidelines. * Week 6 describes data design terms, concepts, and skills including entity-relationship diagrams, cardinality, data normalization rules, data warehousing, data mining, a comparison of logical and physical records, and data control measures.   **Practice Day:**  System Design Engineering: students continue to work on their projects and designing (user interface design, data design, forms and reports design) the system. And finalizing Technical Specification Report. |
| 7 | **System Programming/Development:** Development and Implementation of the system | * provide an overview of the system implementation process * describe how software applications are planned before starting to develop the system * chose system programming/developing method/methodology and start to develop the system * list the deliverables for documenting the system and for training and supporting users * explain why system implementation sometimes fails   Week 7 includes coverage of application development and implementation topics, including structure charts, documentation techniques, system testing, user training, data conversion, changeover methods, and post-implementation evaluation.  **Practice Day:**  System Programming/Developing/Coding: students continue to work on their projects and starting to develop/programming the system (according to Technical Specification Report). |
| 8 | **Components of Cloud Computing.**  **Cloud Computing Service and Deployment Models** | * Overview of Cloud Infrastructure * Virtualization and Virtual Machines * Types of Virtual Machines * Bare Metal Servers * Secure Networking in Cloud * Overview of Service Models * IaaS – Infrastructure as a Service * PaaS – Platform as a Service * SaaS – Software as a Service * Public Cloud * Private Cloud * Hybrid Cloud   In this week, you will learn about the different types of service and deployment models of cloud computing. You will learn about the various components of a cloud computing architecture, such as virtualization, virtual machines, bare metal servers, and the difference between virtual machines and bare metal servers. You will learn how to build a secure cloud networking presence and how container-based technologies work. |
| 9 | **Blockchain Fundamentals** | * What is Blockchain * Centralized vs. Decentralized Systems * Layers of Blockchain * The Business context of Blockchain * Example of Blockchain Networks   In this week, you will learn the theory behind Blockchain. |
| 10 | **System Testing: Quality Assurance - System Test Management.** | * Test Strategy Overview * Integration Testing * Performance Testing * Migration Testing * Security Testing (Penetration Testing)   **Practice Day:**  Students projects discussion day. Test Management: students starts to preparing use cases and test cases according to test stages/phases (Integration, User Acceptance, Penetration). And students preparing manual and automated test cases. |
| 11 | **System Testing: Quality Assurance - System Defect Management.** | Test Defect Management Overview  Defects Severity (Critical, Major, Minor, Suggested) |
| 12 | **Individual Seminar (Individual Research Report)** | 20 min. for each student (including PowerPoint presentation + Research Report) |
|  | **Final Exam** |  |

**Instructor of the course \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Head of the department \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

* **List of Information Security Individual Semester Projects**:

Here is a list of individual semester project ideas for a Systems Analysis and Design course that focus on information security using real-world case studies:

1. **Data Breach Analysis and Prevention (Data Breach Mitigation Plan):** Select a recent real-world data breach case (e.g., Equifax, Target, or Sony) and analyze the security flaws that led to the breach. Analyze a real data breach case and develop a mitigation plan to prevent future breaches. Develop a system design that addresses these vulnerabilities and proposes preventive measures.
2. **Healthcare Data Security (Healthcare Data Security Compliance/ Framework) (Banu, Gultac):** Explore a healthcare data breach case (e.g., Anthem or Premera Blue Cross) and design a secure health information system, considering HIPAA compliance, data encryption, and access control. Develop a security framework for protecting healthcare data, inspired by a case involving healthcare data breaches.
3. **E-commerce Platform Security (E-commerce Platform Vulnerability Assessment, E-commerce Website Security Enhancement) Aynura, Milano, Esmira:** Choose a case study involving a security incident in an e-commerce platform (e.g., eBay or Shopify). Enhance the security of an e-commerce website based on a case study of an e-commerce platform's security flaws. Design a secure e-commerce system with robust payment processing and user data protection features.
4. **Government Cyberattack Response System (Government Agency Cybersecurity Strategy, Government Cybersecurity Incident Re0sponse) (Ayxan K., Samral):** Investigate a real-world cyberattack against a government agency (e.g., a DDoS attack on government websites). Develop a comprehensive cybersecurity strategy for a government agency, influenced by a case of a government cyberattack. Develop a system for detecting, responding to, and mitigating such attacks.
5. **Social Media Privacy (Social Media Privacy Controls) (Ayxan M., Ravan, Seymur):** Analyze a case related to a social media platform's privacy breach (e.g., Facebook or Twitter). Design a privacy-focused social media platform with secure user authentication and data protection. Design enhanced privacy controls for a social media platform inspired by privacy breaches and data misuse incidents.
6. **Secure Online Banking System (Secure Mobile Banking App Design):** Design a secure mobile banking application based on a case study involving mobile banking vulnerabilities. Study a case involving a cyberattack on an online banking system. Design a secure online banking platform that addresses vulnerabilities and safeguards financial transactions.
7. **Ransomware Incident Recovery (Ransomware Incident Response Plan):** Research a ransomware attack case and create a system that helps organizations recover from such attacks, including data decryption and incident response. Create a ransomware incident response plan based on a real ransomware attack case.
8. **Insider Threat Detection System:** Investigate a case of insider threats leading to data leaks (e.g., Edward Snowden). Design a system that monitors and detects suspicious user activities within an organization. (Design a system for detecting insider threats within an organization, inspired by a case of insider data breach.)
9. **Critical Infrastructure Security Design:** Explore a case involving a cyberattack on critical infrastructure (e.g., the Stuxnet attack on Iran's nuclear program). Develop a system for securing critical infrastructure against cyber threats. (Develop a security design for protecting critical infrastructure systems after analyzing a case of critical infrastructure cyberattack.)
10. **Secure Cloud Migration Strategy:** Choose a case study where an organization successfully migrated to the cloud securely (e.g., Netflix or NASA). Develop a comprehensive cloud migration strategy with security considerations. (Design a secure cloud migration strategy influenced by a successful cloud migration case.)
11. **Securing Remote Work Environments (Remote Work Security Framework):** Analyze cases of security incidents related to remote work environments (e.g., the SolarWinds breach). Design a secure remote work system with strong access controls and monitoring. (Create a framework for secure remote work based on a case study involving remote work security vulnerabilities.)
12. **IoT Security (Nihat, Saleh):** Investigate a case of IoT device vulnerabilities leading to security breaches (e.g., Mirai botnet). Design a secure IoT ecosystem, addressing device authentication and firmware updates. (Design a secure Internet of Things (IoT) device and system. Address issues like authentication, data encryption, and secure communication for IoT devices.)
13. **Secure Supply Chain Management:** Study a case involving supply chain cyberattacks (e.g., SolarWinds or NotPetya). Design a secure supply chain management system with enhanced security checks.
14. **Secure Elections System:** Analyze a case related to election security (e.g., concerns about the security of electronic voting systems). Design a secure electronic voting system with transparency and auditability after analyzing concerns about election security.
15. **\* Securing Educational Technologies (Elnur, Shalala, Jamila):** Investigate a case of cybersecurity issues in educational technologies (e.g., Zoom security concerns). Design a secure online education platform with privacy protections.
16. **Identity and Access Management (IAM) Solution:** Design an IAM solution for an organization after analyzing a case of identity theft.
17. **Healthcare Data Privacy Platform:** Design a secure platform for healthcare data storage and sharing, inspired by cases involving healthcare data privacy breaches.
18. **Security Evaluation of a Cloud Service (Raqsana, Khalida, Gulay):** Analyze the security features and potential risks of a cloud service (e.g., AWS, Azure, Google Cloud). Provide recommendations for securing data and applications hosted on the service.
19. **Secure Data Backup and Recovery Strategy:** Design a robust data backup and recovery strategy for an organization, ensuring data integrity, availability, and confidentiality.
20. **Security Awareness Training Platform:** Develop an e-learning platform for security awareness training. Include modules on phishing, social engineering, and best practices in cybersecurity.
21. **Cryptocurrency Security:** Research and present (design) a comprehensive overview of cryptocurrency security, including wallet security, smart contract vulnerabilities, and blockchain consensus mechanisms.
22. **Mobile App Security Assessment (Turane, Asmar, Elcan):** Choose a mobile application, analyze its security features, and identify potential security flaws. Suggest improvements or develop a prototype for a more secure version.
23. **Blockchain-Based Security:** Explore how blockchain technology can enhance security in a specific domain, such as supply chain management or healthcare records. Design and Develop a prototype or whitepaper outlining the use of blockchain.
24. **Social Engineering Awareness Campaign (Elmir):** Create an awareness campaign to educate employees or users about social engineering attacks. Design and Develop materials like posters, training modules, and simulated phishing campaigns.
25. **Secure Software Development Lifecycle (SDLC):** Design and document a secure SDLC process for a software development organization. Include security checkpoints, testing phases, and integration with agile or DevOps practices.
26. **Cybersecurity Incident Simulation:** Design and Develop a simulated cybersecurity incident scenario and conduct tabletop exercises to test an organization's incident response capabilities.