Curriculum Development at Princess Sumaya University for Technology

Overview

The Master's program in Cybersecurity (until now Masters in Information Systems Security and Cyber Crimes) at Princess Sumaya University for Technology has substantially revised its curriculum. This update is part of the ELEGANT project, which aims to enhance university-enterprise cooperation in Jordan and Lebanon. The project focuses on improving students' teaching and learning experience and increasing their employability by addressing the gap between current academic offerings and the needs of the ICT industry.

Curriculum Changes

Updating Course Descriptions:

The course descriptions have been thoroughly revised to reflect current trends and practices in cybersecurity. For instance, the course on "Digital Forensics Investigation" now emphasizes proficiency in investigating cybercrimes and understanding legal frameworks. At the same time, "Secure Software Development" focuses on integrating security practices into the software development lifecycle.

Addition of New Courses:

New courses have been introduced to the curriculum to equip students with up-to-date knowledge and skills. These courses include "Advanced Digital Forensics" and "Wireless and Mobile Security," reflecting the evolving landscape of cybersecurity challenges and technologies.

Deletion of Outdated Courses:

As part of the curriculum update, some courses have been removed. These deletions reflect a strategic shift towards more relevant and contemporary content that aligns with industry needs. The deleted methods are not explicitly listed in the provided document, but their removal is part of the overall strategy to modernise the curriculum.

Objective

These changes are designed to provide students with an advanced understanding of cybersecurity, equipping them with the necessary skills to tackle real-world challenges. The curriculum is updated to ensure that graduates possess both the theoretical knowledge and practical skills desired by employers in the dynamic field of ICT.

Significance

This curriculum update is a strategic step towards bridging the gap between academic knowledge and industry requirements. By aligning the coursework with the latest industry trends and demands, the Information Systems Security and Cyber Crimes program aims to significantly enhance the employability of its graduates, preparing them for successful careers in the rapidly evolving field of cybersecurity.

Detailed Description of Curriculum Update

Updated courses:

The update table presented is a structured outline of new courses introduced to a Cybersecurity program at PSUT. It contains a list of ten courses, each with a unique course number, a descriptive name, and a detailed description of the course content.

1. 15711: Digital Forensics Investigation (DFI) - This course focuses on the fundamentals of addressing cybercrimes, covering evidence collection, data retrieval, and crime reporting.
2. 15760: Secure Software Development - It teaches secure integration of security measures into software development, including lifecycle models, secure coding, and industry best practices.
3. 15720: Advanced Network Security - This is an in-depth exploration of network security, delving into concepts like IP security, wireless security, and network attack analysis.
4. 15751: Ethical Hacking Techniques - The course trains students in ethical hacking, learning about reconnaissance, system scanning, and defense strategies against hacking.
5. 15713: Advanced Digital Forensics - Offering a deep dive into digital forensics, it covers legal and ethical aspects, evidence handling, and analysis techniques across various platforms.
6. 15721: Wireless and Mobile Security - This covers securing wireless networks and mobile devices, with a focus on security protocols and mobile application security.
7. 15781: Information Systems Risk Management - This course introduces risk management in information systems, including risk identification, assessment, and mitigation strategies.
8. 15792: Special Topics in Cybersecurity - A course that adapts to the evolving landscape of cybersecurity, covering the latest advances and methodologies.
9. 15790: Seminar - Designed to provide an understanding of the research process in cybersecurity, this course emphasizes critical thinking and analytical research skills.
10. 15791: Project - A capstone project course that allows students to conduct individual studies, showcasing their research and analytical capabilities in information systems security.

Each course description is designed to offer a comprehensive understanding of the respective topic, ensuring students are well-equipped with current knowledge and practical skills relevant to the field of cybersecurity.

Deleted Course :

1. 11768: OS and file systems Forensic Analysis - Focuses on the configuration of secure operating systems and includes practical problem-solving exercises relevant to work environments.
2. 11769: Cryptography - Covers cryptographic techniques and analysis, including symmetric and asymmetric encryption, as well as cryptanalytic attacks.
3. 11781: Cyber Law and Crime Fundamentals - Examines the legal aspects of online crime and the evolution of criminal law in the context of new technology developments.
4. 12782: Forensics Expert in Courtroom - Offers hands-on experience with the development and presentation of computer evidence testimony in legal settings.
5. 11765: Biometrics - Introduces biometric technologies for personal identification and discusses their potential as successors to traditional PIN systems.
6. 11732: Information Security - Covers the fundamentals of information security, including security architectures, various security controls, and secure applications.
7. 11784: Information System Auditing - Focuses on the foundations of auditing information systems, including the audit process and the technologies and regulations involved.
8. 11789: IT Project Management - Discusses the characteristics of IT projects and project management techniques, with an emphasis on managing scope, time, cost, and quality.
9. 11787: Disaster and Crises Management - Addresses disaster recovery and emergency planning in corporate information systems, including risk evaluation and contingency planning.

New courses

1. 15710 Advanced Cryptography - Delving into the mathematical principles of cryptography for network security, including symmetric and asymmetric encryption, cryptanalysis, and post-quantum cryptography.

2. 15750 Cyber Threat Intelligence - Introducing computational intelligence techniques for system defense and anomaly detection, including AI and machine learning applications in threat hunting.
3. 15714 Advanced Data Integrity and Authentication - Offering an in-depth look at ensuring data accuracy and authentication, covering everything from error-correcting codes to advanced protocols like Zero-knowledge proofs.
4. 15715 Blockchain Technology - Providing foundational knowledge of blockchain and its applications in various industries, with a focus on design, implementation principles, and use cases.
5. 15722 Cloud Computing Security - Covering the challenges of securing cloud computing environments and big data systems, including best practices and security controls.
6. 15723 Multimedia Security - Addressing security and privacy in multimedia content, including steganography, watermarking, and deep fake detection.
7. 15730 Malware Reverse Engineering - Introducing techniques for malware analysis and reverse engineering, including both static and dynamic analysis methods.
8. 15732 Introduction to Hardware Security and Trust - Investigating security and trust issues in hardware design and operation, with a focus on threats like hardware Trojans and countermeasures.
9. 15733 Cyber-Physical Systems and Security - Offering a comprehensive introduction to cyber-physical systems, including design and security considerations.
10. 15784 Cyber Resilience and Business Continuity - Teaching the principles and best practices for maintaining business continuity and resilience in the face of cyber incidents.

11. 15793 Current Emerging Trends in Cybersecurity - Exploring the latest information security trends, preparing students for the evolving challenges in the field.

Each course is designed to equip students with the knowledge and skills necessary to address specific aspects of cybersecurity, from the technical intricacies of cryptography to the strategic planning required for business continuity. The curriculum reflects a broad and deep approach to cybersecurity education, aiming to prepare students for a variety of roles within the field.

The amendments detailed in this document reflect a comprehensive update to the Master's program in Cybersecurity, aligning the curriculum with the latest industry standards and academic research. The new version of the program, as outlined, incorporates these changes and represents a forward-thinking approach to cybersecurity education.