BACHELOR OF SCIENCE IN CYBER SECURITY

Specialization   **Security of Information and Communication Systems**

The field of Cyber Security is evolving rapidly as new risks and threats emerge. From private corporations to government entities, cyber security specialists play a role in the development of network security systems and protocols that ensure the protection of our most vital data. NURE's Bachelor of Science in Cyber Security degree program offers students the opportunity to gain the fundamental expertise which can be useful in a career in this field.

Students who enroll in the Bachelor of Science in Cyber Security program start their learning with general education courses such as: Mathematical Analysis; Physics; Number Theory; Theory of Groups, Fields and Rings; Elliptic Curves; Discrete Mathematics; Probability Theory & Math Statistics; Information and Communication Systems; Information Theory and Coding.

From there, they move on to the core areas of their degree program.

CORE MODULES:

Cryptography and Cryptology

This module provides an introduction to the fundamental components of encryption. Topics include the methods and algorithms of cryptography, symmetric encryption, public-key encryption systems, digital signature schemes and cryptographic protocols.

Elements of Computing and Programming

This module covers three related themes of computer architecture, operating systems and networks. Aspects of computer security are discussed appropriately within the topics. Topics include processes, file systems, memory management, and shell scripting. This module also covers general programming skills and applies them to the widely-used programming languages (C / C++ / C # / Java / PHP / Python and etc.). During the period of study, students learn basic disciplines in programming: programming technology, object-oriented programming, programming of basic objects of information security.

Operating Systems and Mobile Device Security

This module explores secure base operating systems on server, desktop, virtual, and mobile platforms. Topics include the practical application of security tools, utilities, and configurations for protecting computer operating systems at both the user and corporate level. Module subject is also related to protecting stand-alone and virtualized servers, cloud computing security, and the protection of mobile platforms such as smart phones, tablets and handheld computers.

Data/Database Security

This module introduces the concept of database security to include: Database Architecture, Password Policies, Auditing, Privileges, and Roles Administration. Emphasis is placed on areas unique to data and database security.

Web, e-Commerce and Application Security

This module explores securing core technologies that support Internet applications and e-commerce. Processes for creating and administering Internet websites to ensure proper protections are introduced. The module also addresses securing applications on Internet websites and mobile platforms, and introduces basic methods for secure development.

Network Security

This module introduces the goals, functional processes, tools, and techniques associated with network security. Services such as firewalls, intrusion detection mechanisms and Virtual Private Networks (VPNs) will be studied. Students will develop an understanding of

telecommunications and networks security protocols used to prevent, detect, and correct potential vulnerabilities associated with both the outsider and insider threats.

Introduction to Cyber Threats, Cyber Investigations and Forensics

This module examines basic methods of investigation, information acquisition and management of Internet and computer forensic cases. Topics include record-searching, note taking and report writing, and using scientific methodology in Cyber investigations. Coverage also includes basic tools and techniques for forensic analysis of computers, networks systems, and mobile devices.

Resources, opportunities

The quality of our teaching and learning environment is obvious not only within courses, but also in resources for high-quality education provided by our University. The educational process takes place in the computer classes, laboratories, which are equipped with up-to-date technics. Students work with telecommunication and computer equipment of such companies as: Intel, Cisco.

JOBS & CAREERS

The roles and job titles in the security sector often involve somewhat overlapping responsibilities, and can be broad or specialized depending on the size and special needs of the organization. As the cybersecurity domain expands and develops further, new roles and titles are likely to emerge, and the roles attributed to the current titles will likely crystallize or evolve.

Jobs in the field of information security: Security Specialist; Security Analyst; Security Engineer; Security Consultant; Security Auditor; Security Manager; IT Project Manager; Security Architect; Security Director; Cryptographer; Cryptanalyst, Forensics Analyst, Source Code Auditor, Penetration Tester, Vulnerability Assessor, Forensics Expert.

IT jobs that can lead to cyber security careers include: Computer Software Engineer, Database Administrator, Network Administrator, Network Engineer, System Administrator, Web Administrator.