MPE2022 CYBER SECURITY & CYBER LAWS (3-0-0)

Course Objectives:

The objectives of the course are to:

- To understand basic cyber security concepts, network fundamentals, and cryptographic techniques.
- To identify common cyber threats, attacks, and system vulnerabilities.
- To learn essential defense and mitigation methods used to protect systems.
- To gain foundational skills in cyber forensics, including data acquisition and analysis.
- To understand cyber laws, the IT Act 2000, and legal and ethical issues related to emerging technologies.

Module I

Cyber Security Fundamentals: Network and security concepts, Information Assurance fundamentals, Basic cryptography, Symmetric and Asymmetric encryption, Public key encryption, Domain Name System (DNS), Firewalls, Virtualization, and Radio-Frequency Identification (RFID).

Module II

Threats and Vulnerabilities: Types of threats: Malware, Phishing, Ransomware, Adware, Spyware, Trojans, Viruses, Worms, Man-in-the-Middle attacks, Scareware, Distributed Denial-of-Service (DDoS) attacks, Rootkits, and Click-fraud. Vulnerabilities-Shellcode, Integer overflow vulnerabilities, Buffer overflows, and SQL injection.
Defense and Mitigation Measures: Anti-virus scanners, static and dynamic analysis methods, anti-analysis techniques, detecting and preventing obfuscation, and identifying run-time attacks.

Module III

Cyber Forensics: Memory and network forensics for Windows and Linux internals, forensic tools, OS hardening, RAM dump analysis, data acquisition and extraction, volatility analysis for OS artifacts and related information, Automated malicious code analysis.

Module IV

Cyber Laws and Legal Framework: Cybercrime and the global legal landscape, IT Act 2000 and its amendments, limitations of the IT Act 2000, cybercrimes and punishments, legal and ethical aspects related to new technologies: AI/ML, IoT, Blockchain, Darknet, and Social Media, cyber laws of other countries, and relevant case studies.

Course Outcomes:

At the end of the course, the student will be able to:

1. Understand the fundamentals of cyber security.
2. Identify and evaluate cyber security threats and vulnerabilities.
3. Apply suitable security techniques and policies to protect systems and information.
4. Recognize common design trade-offs in developing secure information systems.
5. Use cyber laws and standards to improve information security and system protection.

Books:

1. Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives - N. K. Ghosh, McGraw-Hill.
2. Cryptography and Network Security: Principles and Practice - William Stallings, Pearson.
3. Computer Security: Principles and Practice - William Stallings & Lawrie Brown, Pearson.

Reference Books:

1. Practical Malware Analysis - Michael Sikorski & Andrew Honig, No Starch Press.
2. Incident Response & Computer Forensics -Jason Luttgens, Matthew Pepe & Kevin Mandia, McGraw-Hill.
3. The Art of Memory Forensics - Michael Hale Ligh, Andrew Case, Jamie Levy &AAron Walters, Wiley.
4. Cyber Law in India -Farooq Ahmad.
5. Network Security Essentials - William Stallings, Pearson.