CP5076 **CYBER SECURITY** **L T PC**
3 0 0 3

OBJECTIVES:

- To understand the nature of threats and cyber security management goals and technology
- To understand the landscape of hacking and perimeter defense mechanisms
- To develop strategies for cyber security and protecting critical infrastructure
- To understand policies to mitigate cyber risks
- To understand the IT Act, scheme, amendments and emerging cyber law and desired cyber ecosystem capabilities

UNIT I OVERVIEW OF CYBER SECURITY 9

Introduction – Cyberspace – Cyber Crime – Nature of Threat – Cyber security – Policy, Mission and Vision of Cyber security Program. Cyber security management system – goals, technology categories – perimeter defense and encryption. Cyber security management framework.

UNIT II ATTACKS AND COUNTERMEASURES 9

Malicious Attacks, Threats, and Vulnerabilities – Scope of cyber-attacks – Tools used to attack computer systems – security breach – Risks, vulnerabilities and threats. Malware – malicious software attack – social engineering attack – wireless network attack – webapplication attack – Countermeasures– Types of Network Security Devices –Firewalls, Intrusion Detection Systems, Content Filtering, Virtual Private Networks – Encryption

UNIT III STRATEGIES FOR CYBER SECURITY 9

Creating a Secure Cyber, Types of Attacks, Comparison of Attacks, Creating an Assurance Framework, Encouraging Open Standards, Strengthening the Regulatory framework, Creating Mechanisms for IT Security, Securing E-Governance Services, and Protecting Critical Information Infrastructure. Areas for Intervention – Legal Responses – Harmonization of Legislation – Criminalization of Cyber Offences – National Security and issues related to Privacy and Freedom of Expression – Investigation Procedures – International Cooperation – Electronic Evidence – Liability of ISPs–Recommendations

UNIT IV POLICIES TO MITIGATE CYBER RISK 8

Promotion of R&D in Cyber security – Reducing Supply Chain Risks – Mitigate Risks through Human Resource Development – Creating Cyber security Awareness– Information sharing – Implementing a Cyber security Framework. Signatures– Digital Signature, Electronic Signature

UNIT V CRITICAL INFORMATION INFRASTRUCTURE PROTECTION 10

National Security – Information Sharing and Coordination – Innovation In Regulatory Approach – Innovation in Security Programs – Proactive Threat and Vulnerability Management – Promoting Best Practices in Critical Infrastructure Sectors – Assessing and Monitoring Security Preparedness of Sectors (Security Index) – Security in Information Technology Supply Chain – Taking Leadership and Participating in International Efforts – Capacity Building in Security Skills and training and Awareness. The Indian Cyberspace– Cyber Threats – Need for a Comprehensive Cyber Security Policy – Need for a Nodal Authority – Need for an International Convention on Cyberspace – Cyber War – Fifth Domain of Warfare – Meeting the Cyber Warfare Challenges.

TOTAL: 45 PERIODS

OUTCOMES:

- Gain knowledge on the nature of threats and cyber security management goals and framework
- Knowledge on the landscape of hacking and perimeter defense mechanisms
- Ability to differentiate and integrate strategies for cyber security and protecting critical infrastructure
- Able to understand policies to mitigate cyber risks
- Knowledge on IT Act, and amendments, copy rights, IPR and cyber law to deal with offenses.

REFERENCES:

1. David Kim and Michael G. Solomon, Fundamentals of Information Systems Security, Third Edition Transition Guide, Jones &Bartlett Learning, 2018.
2. Peter Trim and Yang – Im Lee, —Cyber Security Management- A Governance, Risk and Compliance Framework, Gower Publishing, England 2014.
3. Institute for Defence Studies and Analysis Report, India's Cyber Security Challenge, 2012 https://idsa.in/system/files/book/book_indiacybersecurity.pdf
4. John G. Voeller, Cyber Security, John Wiley & Sons, England, 2014.
5. Carol C. Woody, Nancy R. Mead, Cyber Security Engineering: A Practical Approach for Systems and Software Assurance, Addison-Wesley, 2016.
6. Edward Griffor, Handbook of System Safety and Security, Syngress an Elsevier Publications, 1st edition, 2017.
7. Thomas A. Johnson Cyber Security- Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare, CRC Press, 2015.
8. NIST Cyber security Framework, Version 1.0, 2014.
9. CGI, —Cyber security in Modern Critical Infrastructure Environments, 2014.
10. Stuart Broderick J, Cyber Security Program, Cisco Security Solutions, June 2016.

CO	PO						PSO		
	1	2	3	4	5	6	1	2	3
1.	√		√					√	
2.	√		√				√	√	
3.	√		√	√		√	√	√	√
4.	√		√	√	√			√	√
5.	√		√	√	√			√	√

CP5087 SOFT COMPUTING LT P C
3 0 0 3

OBJECTIVES:

- To learn the key aspects of Soft computing and Neural networks.
- To study the fuzzy logic components.
- To gain insight onto neuro fuzzy modeling and control.
- To know about the components and building block hypothesis of genetic algorithm.
- To gain knowledge in machine learning through neural networks.

UNIT I INTRODUCTION TO SOFT COMPUTING 9

Evolution of Computing – Soft Computing Constituents – From Conventional AI to Computational Intelligence – Machine Learning Basics