BACHELORS WITH INFORMATION TECHNOLOGY AS MAJOR (CT – III)

6th SEMESTER

BIT622J3 INFORMATION TECHNOLOGY _ CYBER SECURITY

CREDITS: THEORY-04; TUTORIA-02

THEORY (4 CREDITS)

UNIT I

Overview of Cyber Security: Definition of Cyber Security and its importance in the modern digital landscape.
Evolution of Cyber Threats: Historical perspective on cyber-attacks and their impact on individuals, organizations, and governments.
Cyber Security Frameworks: Introduction to NIST Cybersecurity Framework, ISO/IEC 27001, and other relevant standards.

UNIT II

Cyber Threats and Attack: Cyber Threats and Attack Vectors, Types of Cyber Threat Actors: State-sponsored attackers, hacktivists, cybercriminals, and insider threats. Common Cyber Attack Vectors: Phishing, malware, ransomware, DDoS (Distributed Denial of Service), and social engineering.
Case Study: WannaCry Ransomware (2017).

UNIT III

Introduction to Cryptography: Encryption Basics: Symmetric and asymmetric encryption algorithms and their applications. Hashing: Understanding cryptographic hash functions and their role in data integrity. Public Key Infrastructure (PKI).
Cyber Defense and Risk Management: Cyber Defense Strategies,
Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS): Technologies to monitor and prevent unauthorized access. Antivirus and Endpoint Protection: Protecting individual devices from malware and cyber threats.
Case Study: SolarWinds Supply Chain Attack (2020).

UNIT IV

Cyber Defense and Risk Management: Cyber Defense Strategies, Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS): Technologies to monitor and prevent unauthorized access. Antivirus and Endpoint Protection: Protecting individual devices from malware and cyber threats. Incident Response and Handling: Incident Detection and Analysis: Identifying and analyzing security incidents promptly. Incident Response Plan: Developing a structured approach to respond to cyber incidents. Risk Assessment and Management: Risk Analysis: Identifying potential threats, vulnerabilities, and potential impact on an organization.
Case Study: Colonial Pipeline Ransomware Attack (2021).

TUTORIAL (2- CREDITS)

Note: The Tutorial Component shall be based on the Unit-I to Unit-IV

REFERENCES:

- Allan Friedman and P. W. Singer, Cyber Security and Cyber war: What Everyone Needs to Know by Published Oxford University
- Don Franke, Cyber Security Basics: Protect Your Organization by Applying the Fundamentals by Publisher CreateSpace Independent Publishing Platform, 2016
- Cybersecurity - Attack and Defense Strategies" by Yuri Diogenes and Erdal Ozkaya, Publication House: Packt Publishing, 2018, Edition: 1st Edition.
- Introduction to Cybersecurity: Stay Safe Online" by Tim Patrick, Apress 1st Edition, 2017