34642 – INFORMATION SECURITY

DETAILED SYLLABUS

UNIT I Overview of information security

1.1 **Introduction:** History of Information Security- critical characteristics of information

1.2. **NSTISSC security model:** Components of Information System- Securing components

1.3 **Balancing information security and access**: Approaches to information security implementation – SDLC – Security System Development Life Cycle – SDLC and SecSDLC phase summary.

UNIT II SECURITY INVESTIGATION

2.1. **Need for security:** Business needs- threats: definition- categories of threats

2.2. **Attacks**: Definition- types of attacks

2.3. **Secure software development**: Software assurance – software design principles software development security problems

2.4 **Law and ethics in information security**: International Laws and legal bodies – ethics and information security- codes of ethics and professional organizations.

UNIT III SECURITY ANALYSIS

3.1. **Risk Management- overview- Risk Identification**: Asset identification – vulnerability identification

3.2. **Risk Assessment:** Introduction-likelihood-risk determination-possible controls

3.3. **Risk Control Strategies**: Selecting a risk control strategy - qualitative verses quantitative risk control practices

3.4 **Risk management discussion points**: Recommended risk control practices

UNIT IV SECURITY TECHNOLOGY

4.1. Firewalls: Introduction- processing modes- firewall architectures – selecting the right firewall- content filters

4.2. **VPN:** Introduction- transport mode- tunnel mode

4.3**. Intrusion Detection and Prevention Systems (IDPS):** Types- IDPS detection methods

4.4. Cryptography: introduction- cipher methods- cryptographic algorithm scryptographic tools

UNIT – V PHYSICAL SECURITY

5.1 **Introduction:** Physical Access Control-Major physical security controls

5.2 **Fire Security and Safety**: Introduction – Fire detection and response

5.3 **Failure of supporting utilities and structural collapse**: Heating, ventilation and air conditioning- power management and conditioning

5.4 **Interception of data**: Mobile and portable system – Special considerations for physical security threats.

Text Book:

1. Handbook of Information Security Management Micki Krause, Harold F Tipton Vol 1-3 CRC Press LLC 2004
2. Principles of Information Security Michael E Whiteman and Herbert J Mattord Vikas Publishing House, NewDelhi 2012