# CYBER CRIMES AND INVESTIGATION

**Course Code:** 15CS2209

| L | P | C |
|---|---|---|
| 3 | 0 | 3 |

**Pre requisites:** Network security

**Course Outcomes:**

By the end of the course

**CO1:** The Student will gain the knowledge on various security threats and issues and how to overcome those issues.

**CO2:** The student will get the capability to analyze various cyber crimes.

**CO3:** Learning various issues involved in threats overcome methods.

**CO4:** Learning Forensic analysis and risk analysis.

**CO5:** Learn inner investigation models for overcoming cyber crimes

**UNIT–I** (10-Lectures)

The State of threats against computers, and networked systems, Overview of computer Security and why they fail Vulnerability assessment, managing firewalls and VPNs, Overview of Instruction Detection and Intrusion prevention Network and host-based IDS. Classes of attackers, Kids/ hackers/ sophisticated groups, automated: Drones, Worms and Viruses A general IDS model and taxonomy.

**UNIT–II** (10-Lectures)

Information security risk analysis fundamentals Importance of physical security and biometrics controls for protecting information systems assets, Security considerations for the mobile work force, Network security perspectives, networking and digital communications (Overview only), security of wireless networks.

**UNIT–III** (10-Lectures)

Security models and frameworks and standards through introduction to the ISO 27001, SSECMM (systems security engineering – capability

maturity model), COBIT (Control Objectives for Information and related technologies) and the Sarbanes-Oxley Act (SOX) and SAS 70 (statement on auditing standards)**,** Privacy Fundamentals, business practices, impact on data privacy, technological impact on data privacy, privacy issues in web services and Applications based on web services.

**UNIT–IV** (10-Lectures)

Internet/Computer Demographics: Computer/network user statistics; Computer crime statistics. Types of Computer and Internet Crime: Types of crimes involving computers; Computer crimes; Network crimes; Criminals, hackers, and crackers

**Investigations:** The investigation life cycle; Legal methods to obtain the computer; Jurisdictions and agencies; Internet investigations (e-mail, IRC, chat rooms, etc.); IP addresses and domain names; Investigative methods, Digital Evidence.

**Evidence Collection:** Working with ISPs and telephone companies; Examining computer server, and network logs; Anonymous services.

**UNIT–V** (10-Lectures)

Introduction to Information System Security, Offensive and Defensive Information
Warfare:

**Cyber Crime:** Fraud and Abuse; National Security, Offensive Information Warfare; Privacy Rights, Ethics, Censorship, Harassment.

**Prevention Techniques:** Access Control, Misuse Detection; Vulnerability Monitoring, Security Policy, Risk Management, Incident Handling; Law Enforcement and Cyber Crime, Emerging Concept in Cyber Crime.

**TEXT BOOKS:**

1. Information Systems Security Management by Nina S. Godbole (Wiley India Pvt. Ltd.)

2. Security Engineering by Ross Anderson
3. Information Security Management Handbook by Harold Tpton & Micki Krause (Auerbach Publications).

**REFERENCE BOOKS:**

1. Network Security Essentials: Applications and Standards W. Stallings (Pearson Education)