LL.M. 2ND SEMESTER

OPTIONAL PAPER

CYBER LAWS AND REGULATION OF ARTIFICIAL INTELLIGENCE

CYBER CRIME AND INTERNATIONAL CYBER SECURITY

Paper: 203-E Max. Marks: 100
Credits: 5
Time: 3 Hours

Note:

1. There shall be total Five Units in the question paper.
2. Unit-I shall contain one compulsory question having four parts of five marks each. This question shall be spread over the entire syllabus.
3. There shall be two questions in each Unit i.e. Unit-II to Unit-V.
4. The student is required to attempt four questions by selecting one question from each unit i.e. Unit-II to Unit-V. Each question shall carry twenty marks.

COURSE OBJECTIVES:

- To analyse the general principles of the Cyber Crime.
- To analyse enforcing agencies of the International Cyber Security and Governance.
- To help the students to evaluate the Law relating toInternational Cyber Security and Crime.
- To understand the Law of International Cyber Security and Crime.

UNIT 1

Introduction and General Principles of Cyber Crime

- Cyber Crimes – Meaning, Definition and types of Cyber Crime
- A Brief History of the Internet, Recognizing and Defining Computer Crime, Contemporary Crimes, Computer as Targets of Crime, Contaminants and Destruction of Data.
- Cyberspace and Criminal Behaviour
- Categories of Cyber Crimes : Cyber Crimes against Individual – Cyber Crimes against Property – Cyber Crimes against Government
- Traditional Problems Associated with Computer Crime

UNIT 2

Regulation of Cyber Security and Cyber Crime

- Child Pornography
- Cyber Stalking
- Denial of service Attack
- Virus Dissemination
- Software Piracy
- Internet Relay Chat (IRC) Crime
- Credit Card Fraud, Net Extortion, Phishing etc
- Cyber Terrorism-Violation of Privacy on Internet
- Data Protection and Privacy

UNIT 3

Technical framework of Cyber Crime Investigation

- Firewalls and Packet Filters
- Password Cracking
- Keyloggers and Spyware, Virus and Warms, Trojan and backdoors
- Steganography, DOS and DDOS attack
- SQL injection, Buffer Overflow
- Attack on wireless Networks
- Cyber Crimes and Investigation Procedures
- Computer Forensics and Digital Evidence

UNIT 4

Legal framework of Cyber Crime Investigation

- Cyber Security Techniques- Challenges and Restrictions
- Cyber Security Policies National and International
- International Convention on Cyber space
- Cyber Security: Legal and Compliance Assessment
- International Approach towards Tech Legal Prospects
- UN's Initiative - E-Treaties - Budapest Convention

COURSE OUTCOME:

- ➢ Expert knowledge in Cyber Crime and Cyber Security.
- ➢ Deep Ability to understand the Theoretical Explanation of Cyber Crime at National and International.

- Develop skills against Cyber Crime and Regulations.
- Psychologically assess the Crime and Criminal.
- Conduct Cyber-Crime Investigations.
- Vulnerability faced by Women, Children and Adolescents in Cyber world.
- After completing this Course, One will be able to understand the framework of Cyber regulation and Cyber Crimes.

SUGGESTED READINGS:

1. Justice Yatindra Singh: Cyber Laws, Universal Law Publishing Co., New Delhi
2. Farouq Ahmed, Cyber Law In India, New Era Publications, New Delhi
3. S.R.Myneni: Information Technology Law(Cyber Laws), Asia Law House, Hyderabad.
4. Chris Reed, Internet Law-Text And Materials, Cambridge University Press.
5. Pawan Duggal: Cyber Law- The Indian Perspective Universal Law Publishing Co., NewDelhi
6. Artificial Intelligence, Data Analytics And Cyber Security –Laws & Practice
7. Shackelford, S.J., ‘The Law Of Cyber Peace’, Chicago Journal Of International Law, 2017
8. Goldsmith, J., ‘Cybersecurity Treaties: A Skeptical View’, A Future Challenges Essay, 2011
9. Sander, B., ‘Cyber Insecurity And The Politics Of International Law’, 2017