COURSE CONTENT

CYBER LAWS								
VII Semester: CSE								
Course Code	**Category**	**Hours / Week**			**Credits**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CIA**	**SEE**	**Total**
2476702	**PE**	2	0	0	2	40	60	100
Contact Classes: 45	**Tutorial Classes: Nil**	**Practical Classes: Nil**				**Total Classes: 45**		
Prerequisites: Fundamentals of Operating System, Networks, Internet protocols, Encryption, and Authentication								

Course Overview:

This course provides an understanding of cybercrime, its types, methods, and global and Indian legal perspectives. It covers cyber security laws, cyber ethics, and the Information Technology Act with real-world case studies. Students gain awareness of cyber offenses, ethical responsibilities, and legal remedies in the digital environment.

Course Objectives:

1. To provide foundational knowledge of cybercrime and its impact on information security at national and global levels.
2. To explain categories of cyber offenses, attack methods, and techniques such as social engineering and botnets.
3. To understand the legal framework of cyber laws, the Indian IT Act 2000, its amendments, and related challenges.
4. To promote ethical practices in cyberspace and analyze real-world cybercrime cases for legal and preventive measures.
5. To analyze real-life cybercrime cases, understand their impact, and discuss preventive and legal measures.

Course Outcomes: After Completion of the Course, Students should be able to

1. Understand the fundamentals of cybercrime, its classifications, and legal perspectives, including the Indian IT Act 2000 and global trends.
2. Understand the categories of cybercrimes, methods used by criminals to plan attacks, and social engineering techniques, including cyberstalking, cybercafé crimes, and the role of botnets in cybercrime.
3. Apply knowledge of the Indian IT Act and its amendments to analyze legal issues, digital signatures, and punishment for cybercrimes.
4. Recognize the importance of cyber ethics, norms, and professional responsibilities to ensure safe and ethical use of technology.
5. Analyze real-life cybercrime cases to identify causes, impacts, and possible legal and preventive measures.

UNIT - I

Introduction to Cybercrime: Introduction, cybercrime and information security, who are cyber criminals? Classification of cybercrimes, legal perspectives, cybercrime and the Indian ITA 2000, a global perspective on cybercrimes.

UNIT - II

Cyber offenses: Categories of cybercrime, how criminals plan the attacks, social engineering: classification of social engineering, cyberstalking, cyber cafe and cybercrime, Botnets- the fuel for cybercrime.

UNIT-III

Cybercrime and Cyber Security: The Legal Perspective: Introduction, The Indian IT Act, challenges to Indian Law and cybercrime scenario in India, Digital signature and the Indian IT act, Amendments to the Indian IT Act, cybercrime and punishment, Cyber law, Technology and student – Indian Scenario.

UNIT-IV

Cyber Ethics: Introduction, Cyber Society, dimensions of cyber ethics, cyber ethics by Norms, Laws and regulations, importance of cyber law, signification of cyber ethics.
Ethics in the information society: principles, Participation, people, profession, privacy, piracy, production, power, policy.

UNIT – V

Cybercrimes: Illustrations, examples and case studies: Introduction, Real-life Examples- official website of hacked; emails spoofing Instance, Parliament Attacks, banks lose millions of rupees. Case Studies- Internet time stealing, Indian cyber defamation, online gambling, Intellectual property crime, counterfeit computer hardware, Online Scams – Fake job offers Scams, Lottery scams.

TEXT BOOKS:

1. Cyber Security, Understanding Cybercrimes, computer forensics and legal Perspectives – Nina Godbole, Sunit Belapure, Wiley India. (Chapter 1, 2, 3, 11)
2. Cyber Ethics 4.0, Christoph Stuckelberger, Pavan Duggal, by Glob ethic

REFERENCES:

1. Debby Russell and Sr. G. T Gangemi, "Computer Security Basics (Paperback)", 2nd Edition, O" Reilly Media, 2006.
2. Thomas R. Peltier, "Information Security policies and procedures: A Practitioner's Reference", 2nd Edition Prentice Hall, 2004.
3. Kenneth J. Knapp, "Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions", IGI Global, 2009.
4. Thomas R Peltier, Justin Peltier and John Blackley", Information Security Fundamentals", 2nd Edition, Prentice Hall, 1996

Jonathan Rosenoer, "Cyber law: the Law of the Internet", Springer-Verlag, 1997 6. James Graham, "Cyber Security Essentials" Averbach Publication T & F Group.

ELECTRONIC RESOURCES:

1) **https://en.wikipedia.org/wiki/Information_Technology_Act%2C_2000**
2) **https://i4c.mha.gov.in/acts-and-rules.aspx**
3) **https://en.wikipedia.org/wiki/National_Cybercrime_Reporting_Portal**
4) **https://edurev.in/t/455956/it-law-and-cyber-crime**
5) **https://edurev.in/t/460363/Summary-Cyber-Laws-Safety-And-Security-In-India**

MATERIALS ONLINE:

1. Course template
2. Tutorial question bank
3. Tech talk and Concept Video topics
4. Open-ended experiments
5. Definitions and terminology
6. Assignments
7. Model question paper – I
8. Model question paper – II
9. Lecture notes
10. E-Learning Readiness Videos (ELRV)