S.No. : 387

NPEC 43213

No. of Printed Pages : 04

Following Paper ID and Roll No. to be filled in your Answer Book.

PAPER ID : 43222 Roll No.

B. Tech. Examination, 2026

(Even Semester)

CYBER LAW AND SECURITY

Time : Three Hours] *[Maximum Marks : 60*

Note :– Attempt all questions.

SECTION – A

1. Attempt all parts of the following : 8×1=8

   (a) Explain the concept of cyber space and cyber law.

   (b) What is digital signature?

   (c) Write any four major type of information system with example.

   (d) Explain GDPR.

[P. T. O.

(e) Write the difference between macro viruses and logic bombs.

(f) What is IPR?

(g) In which year was the IT act enacted in India?

(h) Define patent and trademark.

SECTION – B

2. Attempt any two parts of the following : 2×6=12

(a) Discuss information assurance and explain how it differ from infosec?

(b) Discuss in detail about various technology used in cyber world for securing data. Also give examples of threats.

(c) What is infosec and what are the three core principles (CIA triads) it aim to protect.

(d) Describe the ethical issues related to hacking-difference between hacking and cyber crime.

SECTION – C

Note :– Attempt all questions. Attempt any two parts from each questions. 8×5=40

3. (a) Explain the concept of SRA and its importance in information system management.

(b) Explain the concept of software piracy, plagarism and the legal consequences under copyright law.

(c) Discuss public key infrastructure and E-cash. How does E-cash differ from traditional payment methods like credit/debit cards.

4. (a) Discuss the importance of backup strategies, archival storage and disaster recovery planning for infosec.

(b) Explain DoS attack and MITM attacks and provide real world scenario where it occurs.

(c) Explain data protection and privacy issues in cyber space.

5. (a) Describe common vulnerabilities in E-commerce website that attacker exploits. Also define 2FA (two factor authentication).

(b) Explain mobile computing and wireless computing. Also discuss the challenges in mobile device security.

(c) Explain the concept of social engineering attacks that exploit physical security weakness.

6. (a) Explain domain name disputes and legal mechanism (like UDRP) for resolving them.

(b) Discuss copyright issues related to software and digital content.

(c) Describe the role of security frameworks (like NIST, ISO 27001) in designing secure systems.

⌘⌘⌘

6(a) Explain firewall & Types of firewall.