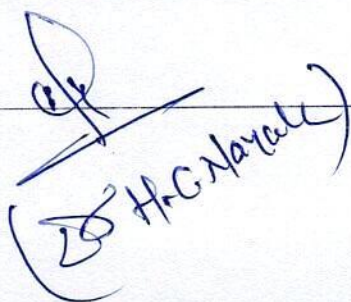


Practical Paper

Part A : Introduction			
Program: Degree with Honours/Research	Class : UG	Year : IV	Session : 2024-2025
Subject: Computer Application			
1.	Course Code	S4-COAP4D	
2.	Course Title	Cyber Security (Theory) (Group B — Paper II)	
3.	Course Type	Discipline Specific Elective (DSE)	
4.	Pre-requisite		
5.	Course Learning Outcomes (CLO)	<ul style="list-style-type: none"> ➤ Give students an extensive overview of cyber security issues, tools and techniques that are critical in solving problems in cyber security domains ➤ Providing concepts of computer security, cryptography, digital money, secure protocols, detection and other security techniques. 	
6.	Credit Value	Theory -4	
7.	Total Marks	Max. Marks: 30+70	Min. Passing Marks: 35
Part B: Content of Course			
Cyber Security			
Total No. of Lectures =60 (In hours per Week) 2-0-0			
Unit	Topics		No. of Lectures
I	Introduction: Cyber Crime, Challenges of cyber crime, Classifications of Cybercrimes: E Mail Spoofing, Spamming, Internet Time Theft, Salami attack/Salami Technique. Web jacking, Online Frauds, Software Piracy, Computer Network Intrusions, Password Sniffing, Identity Theft, cyber terrorism, Virtual Crime, Web servers were hacking, session hijacking. Concept of Cyber Crime and the IT Ac 2008: Introduction of Act, Hacking, Teenage Web Vandals, Cyber Fraud and Cheating, Defamation, Harassment and E-mail Abuse, Other IT Act Offences, Monetary Penalties, jurisdiction and Cyber Crimes.		12
II	Cyber Security Concepts: Essential Terminologies, CIA, Risks, Breaches, Threats, Attacks, Exploits. Information Gathering (Social Engineering, Foot Printing & Scanning). Open Source/ Free/ Trial Tools: nmap, zenmap, Port Scanners, Network scanners.		12
III	Cryptography: Symmetric key Cryptography, Asymmetric key Cryptography, Message Authentication, Digital Signatures, Applications of Cryptography. Overview of Firewalls- Types of Firewalls, User Management, VPN Security, Security Protocols: - security at the Application Layer- PGP and S/MIME, Security at Transport Layer- SSL and TLS, Security at Network Layer-IPSec.		12
IV	System Security: Server Security, OS Security, Physical Security, Introduction to Networks, Network packet Sniffing, Network Design Simulation. DOS/ DDOS attacks. Asset Management and Audits, Vulnerabilities and Attacks. Intrusion detection and Prevention Techniques, Host based Intrusion prevention Systems, Security Information Management, Network Session Analysis, System Integrity Validation.		12
V	Internet Security: Cloud Computing and Security, Social Network sites security, Cyber Security Vulnerabilities-Overview, vulnerabilities in software, System administration, Complex Network Architectures, Open Access to Organizational Data, Weak Authentication, Authorization, Unprotected Broadband communications, Poor Cyber Security Awareness.		12


 (H.G. Nayak)

Part C : Learning Resources
Text Books, Reference Book, Other Resources

Suggested Reading:

1. Cryptography and Network Security by William Stallings (Pearson Education/PHI).
2. Cyber Law Simplified by Vivek Sood (TMH)..
3. Cyber Security by Nina Godbole, Sunit Belapure (Wiley-India).
4. Information and Cyber Security by Gupta Sarika (Khanna Publishing House)
5. मध्य प्रदेश हिंदी ग्रंथ अकादमी की पुस्तकें।

Suggested Digital Platforms, Web-links:

1. <https://archive.nptel.ac.in/noc/courses/220/>
2. <https://www.simplilearn.com/tutorials/cyber-security-tutorial-3>.
3. <https://intellipaat.com/blog/tutorial/ethical-hacking-cyber-security-tutorial/>
4. <https://www.youtube.com/watch?v=lpa8uy4DyMo>
5. <https://www.udemy.com/topic/cyber-security/free/>

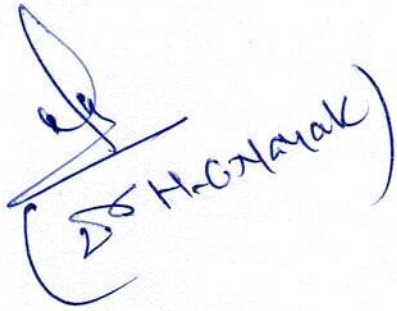
Part D : Assessment and Evaluation

Suggested Continuous Evaluation Methods:

Maximum Marks : 100

Continuous Comprehensive Evaluation (CCE): 30 Marks University Exam(UE): 70 Marks

Internal Assessment: Continuous Comprehensive Evaluation (CCE)	Class Test Assignment / Presentation	30
External Assessment : University Exam Section Time : 03:00 Hours	Section(A): Very Short Questions Section (B): Short Questions Section (C) : Long Questions	70



(H. G. Nayak)

सैद्धांतिक प्रश्नपत्र

भाग ए : परिचय			
कार्यक्रम : ऑनर्स/रिसर्च के साथ डिग्री	कक्षा : यूजी	वर्ष : चतुर्थ	सत्र : 2024-2025
विषय : कंप्यूटर अनुप्रयोग			
1.	पाठ्यक्रम कोड	S4-COAP4D	
2.	पाठ्यक्रम शीर्षक	Cyber Security (Theory) (Group B — Paper II)	
3.	कोर्स का प्रकार	Discipline Specific Elective (DSE)	
4.	पूर्व-आवश्यकता		
5.	पाठ्यक्रम सीखने के परिणाम) सीएलओ(<ul style="list-style-type: none"> ➤ छात्रों को साइबर सुरक्षा मुद्दों ,उपकरणों और तकनीकों का व्यापक अवलोकन दें जो साइबर सुरक्षा डोमेन में समस्याओं को हल करने में महत्वपूर्ण हैं ➤ कंप्यूटर सुरक्षा ,क्रिप्टोग्राफी ,डिजिटल मनी ,सुरक्षित प्रोटोकॉल ,पहचान और अन्य सुरक्षा तकनीकों की अवधारणाएं प्रदान करना। 	
6.	क्रेडिट मूल्य	सिद्धांत4-	
7.	कुल मार्क	अधिकतम .अंक70+30 :	न्यूनतम .उत्तीर्ण अंक35 :
भाग बी : पाठ्यक्रम की सामग्री			
Cyber Security			
व्याख्यानों की कुल संख्या) 60= प्रति सप्ताह घंटों में0-0-2 (
इकाई	विषय	व्याख्यानों की संख्या	
प्रथम	परिचय : साइबर अपराध ,साइबर अपराध की चुनौतियाँ ,साइबर अपराधों का वर्गीकरण :ई मेल स्फूफिंग ,स्पैमिंग ,इंटरनेट टाइम चोरी ,सलामी हमला/सलामी तकनीक। वेब जैकिंग , ऑनलाइन धोखाधड़ी ,सॉफ्टवेयर चोरी ,कंप्यूटर नेटवर्क Intrusions ,पासवर्ड Sniffing , Identity Theft ,साइबर आतंकवाद ,आभासी अपराध ,वेब सर्वर हैकिंग ,session hijacking साइबर अपराध की अवधारणा और आईटी अधिनियम :2008 अधिनियम का परिचय , हैकिंग ,Teenage Web Vandals ,साइबर धोखाधड़ी और धोखाधड़ी ,मानहानि ,उत्पीड़न और ई-मेल दुरुपयोग ,अन्य आईटी अधिनियम अपराध ,मौद्रिक दंड ,क्षेत्राधिकार और साइबर अपराध।	12	
द्वितीय	साइबर सुरक्षा अवधारणाएँ :Essential Terminologies ,CIA ,जोखिम ,उल्लंघन ,धमकी ,हमले ,शोषण। सूचना एकत्र करना)सोशल इंजीनियरिंग ,फुट प्रिंटिंग और स्कैनिंग।(। ओपन सोर्स/फ्री/ट्रायल टूल्स :एनएमएपी ,ज़ेनमैप ,पोर्ट स्कैनर्स ,नेटवर्क स्कैनर्स।	12	
तृतीय	क्रिप्टोग्राफी :Symmetric key क्रिप्टोग्राफी ,Asymmetric key क्रिप्टोग्राफी ,संदेश प्रमाणीकरण ,डिजिटल हस्ताक्षर ,क्रिप्टोग्राफी के अनुप्रयोग। फ़ायरवॉल का अवलोकन - फ़ायरवॉल के प्रकार ,उपयोगकर्ता प्रबंधन ,VPN सुरक्षा ,सुरक्षा प्रोटोकॉल - :एप्लिकेशन लेयर पर सुरक्षा -PGP और S/MIME ,ट्रांसपोर्ट लेयर पर सुरक्षा -SSL और TLS ,नेटवर्क लेयर-IPSec पर सुरक्षा।	12	
चतुर्थ	सिस्टम की सुरक्षा :सर्वर सुरक्षा ,ओएस सुरक्षा ,भौतिक सुरक्षा ,नेटवर्क का परिचय ,नेटवर्क पैकेट Sniffing ,नेटवर्क डिज़ाइन सिमुलेशन। DOS/ DDOS attacks .Asset Management और Audits ,Vulnerabilities और Attacks। Intrusion detection and Prevention Techniques ,Host based Intrusion prevention Systems ,सुरक्षा सूचना प्रबंधन ,नेटवर्क सत्र विश्लेषण ,System Integrity Validation.	12	


 (Dr. H. G. Nayak)

पंचम	इंटरनेट सिक्कूरिटी :क्लाउड कंप्यूटिंग और सिक्कूरिटी, सोशल नेटवर्क साइटों की सिक्कूरिटी साइबर सुरक्षा Vulnerabilities- अवलोकन, सॉफ्टवेयर में Vulnerabilities, सिस्टम प्रशासन, काम्प्लेक्स नेटवर्क आर्किटेक्चर, Open Access to Organizational Data, Weak Authentication, प्राधिकरण, असुरक्षित ब्रॉडबैंड संचार, Poor Cyber Security Awareness.	12
भाग सी :सीखने के संसाधन पाठ्य पुस्तकें, संदर्भ पुस्तक, अन्य संसाधन		
Suggested Reading: 1. Cryptography and Network Security by William Stallings (Pearson Education/PHI). 2. Cyber Law Simplified by Vivek Sood (TMH).. 3. Cyber Security by Nina Godbole, Sunit Belapure (Wiley-India). 4. Information and Cyber Security by Gupta Sarika (Khanna Publishing House) 5. मध्य प्रदेश हिंदी ग्रंथ अकादमी की पुस्तकें। Suggested Digital Platforms, Web-links: 1. https://archive.nptel.ac.in/noc/courses/220/ 2. https://www.simplilearn.com/tutorials/cyber-security-tutorial-3 3. https://intellipaat.com/blog/tutorial/ethical-hacking-cyber-security-tutorial/ 4. https://www.youtube.com/watch?v=Ipa8uy4DyMo 5. https://www.udemy.com/topic/cyber-security/free/		
भाग डी : असेसमेंट और मूल्यांकन		
सुझाई गई सतत मूल्यांकन विधियाँ: अधिकतम अंक 100: सतत व्यापक मूल्यांकन) सीसीई 30:(अंक विश्वविद्यालय परीक्षा) यूई 70:(अंक		
आंतरिक मूल्यांकन: सतत व्यापक मूल्यांकन) सीसीई(Class Test Assignment / Presentation	30
बाहरी मूल्यांकन: विश्वविद्यालय परीक्षा अनुभाग समय 03:00 : घंटे	Section(A): Very Short Questions Section (B): Short Questions Section (C) : Long Questions	70


 (H.C. Nayak)