

(6 pages)

Reg. No.:.....

Code No. : 30204 E Sub. Code : GMCA 62

B.C.A. (CBCS) DEGREE EXAMINATION,
APRIL 2020.

Sixth Semester

Computer Applications — Main

CYBER SECURITY

(For those who joined in July 2012 - 2015)

Time : Three hours

Maximum : 75 marks

PART A — (10 × 1 = 10 marks)

Answer ALL questions.

Choose the correct answer

1. During which phase of the SDLC are users trained to use the new system?
 - (a) preliminary investigation
 - (b) systems implementation
 - (c) systems development
 - (d) systems maintenance

2. After implementation of the system, system maintenance could be done for
 - (a) Minor changes in the processing logic
 - (b) Errors detected during the processing
 - (c) Revision of the formats of the reports
 - (d) All of the above
3. VPN is abbreviated as _____.
 - (a) Visual Private Network
 - (b) Virtual Protocol Network
 - (c) Virtual Private Network
 - (d) Visual Protocol Network
4. Which is/are ways to deal with risk?
 - (a) Contingency
 - (b) Transfer
 - (c) Ignore
 - (d) All of the above
5. An encryption algorithm transforms the plaintext into
 - (a) Cipher text
 - (b) Simple Text
 - (c) Plain Text
 - (d) Empty Text
6. Which of the following is a system designed to attract and identify hackers?
 - (a) Honey pot
 - (b) Firewall
 - (c) Honey trap
 - (d) IDS

7. Lack of access control policy is a _____.
(a) Bug (b) Threat
(c) Vulnerability (d) Attack
8. What type of attack can be performed once a hacker has physical access?
(a) Finding passwords by dumpster diving
(b) Stealing equipment
(c) Performing a DoS attack
(d) Session hijacking
9. _____ comprise a set of rules that dictates acceptable and unacceptable behaviour within an organization
(a) Standards (b) Procedures
(c) Guidelines (d) Policies
10. The _____ programme once installed must be continued on a permanent basis.
(a) Job evaluation
(b) Training and Development
(c) Recruitment
(d) All of the above

PART B — (5 × 5 = 25 marks)

Answer ALL questions, choosing either (a) or (b).

Each answer should not exceed 250 words.

11. (a) Write short notes on threats in Information Security.

Or

- (b) Discuss NSTISSC security model.

12. (a) Explain in detail about Risk Identification.

Or

- (b) Write briefly about Information Security Policy.

13. (a) Write short notes on Access Control Devices.

Or

- (b) Write Short notes on DES Algorithm.

14. (a) Write short notes on Physical Access controls.

Or

- (b) Discuss about Information security Certification and Accreditation.

15. (a) Write short notes on Privacy and Security of Personal Data.

Or

- (b) Illustrate the features of Security Management Models.

PART C — (5 × 8 = 40 marks)

Answer ALL questions, choosing either (a) or (b)

Each answer should not exceed 600 words.

16. (a) Elaborate in detail about different Components of an Information System.

Or

- (b) Explain briefly about Law and Ethics in Information Security.

17. (a) Explain in detail about Risk Management Strategies.

Or

- (b) Discuss in detail about Firewall and VPN.

18. (a) Discuss about Honey Pots, Honey Nets and Padded cell system.

Or

- (b) Discuss any two Cryptographic Algorithms.

19. (a) How physical security implemented in mobile and portable system.

Or

- (b) Discuss in detail about implementation of information Security.

20. (a) Explain the employment policies for IS professional and nonemployees.

Or

- (b) Explain in detail about information Security Maintenance Model.
-