Thematic areas for Master's State Exam for compulsory courses of ICB

Information and communication security

1. Malware history and the most famous malware demos. Danger of malware, examples. Turing machine and Von Neumann autoproduction automata.
   Recursive functions and virus functionality.
2. Cyber war and cyber weapon. Pillar of the War Zone - Explain the position and role of malware. Antimalware rules for correct behavior in the cyberspace.
3. Formal definition of virus, structure, operation and phase. Virus behavior and properties. 7 differences - similarities between computer and biological viruses, building blocks of the virus and their functional order.
4. Malware statistics and malware activity information processing.
5. Virus infections. Methods. Oligomorphism, polymorphism and metamorphism, decryptor, EPO. its functionality and use. Show examples.
6. Virus generator, non-traditional methods of viral code synthesis and mutation.
7. Reverse engineering of the virus, technology and resources.
8. Cryptographic methods and their use in malware (ransomware, ...)
9. Malware dependence on OS, hardware, file system. Reverse compatibility and cross infection.
10. Basic malware defense strategies. Memory scanning, code emulation, obfuscation, data encryption, anti-emulation and anti-heuristic techniques.
11. Resident virus, explain and display schematic principles, stealth virus, schematic principle, stealth techniques.
12. Retrovirus. Technologies and principles.
13. Generic structure of computer worm. Spread f infection. Worm update, interaction between different types of malware. Worms and mobile devices.
14. Payload. Destructive vs non-destructive payload. Examples.
15. Backup and Restore. Backup frequency. Types of backup technologies and sw. Basic Backup Policy.
16. Three levels of the site, explain. Browsers, Search Engines, TOR, DuckDuckGo. Dark vs. deep web. Silk road and wikipedia of the dark web. Bitcoin and the dark web. Cybercrime and Dark Web.
17. Cyberspace. Definition. Computer crime and security. 5 pillars of cyber security.
18. The difference between cyber-security and cybersafety.
19. Vector and phases of cyber attack. Malware and Attack - CnC, DDoS, Botnet. Vulnerability.
20. What are advanced threat protection policies? 10 cybersecurity rules.
21. Blockchain technology and its use.
22. Penetration testing of software applications. Penetrate and patch model and its advantages and disadvantages. White box, black box and gray box testing.

23. Prescriptive and descriptive approach to penetration testing and software development. For each approach, specify and describe a specific example of a framework or standard.
24. Scripting attacks and defense options against these attacks (PowerShell scripts, JavaScript scripts). Specifics associated with scripting attacks, infection vectors, persistent and non-persistent attacks.
25. Input validation problem and injection attacks (SQL injection, XPATH injection, OS command injection).
26. Denial of service attacks and distributed denial of service attacks (DOS, DDOS), types of attack and defense against them.
27. Sensitive application data management (how to work with configuration values, using exceptions and how to display them, etc.), data logging for the needs of automated analysis.
28. Social engineering and phishing. Description of techniques and examples of use.
29. Risk analysis and management. Security audit and standards.
30. Identity and Access Management, Remote Monitoring.
31. Data centers: typical components and standards for their design and use.
32. Securing network of the infrastructure and SAN data center networks.
33. The process of forensic investigation and its phases: Identification, Collection, Preservation, Examination, Analysis, Presentation
34. Searching for clues and securing evidence in Windows OS (Registry, Windows Logs, Processes, etc).
35. Open source intelligence and its use in forensic analysis.

Information and communication technologies

1. Symmetric cryptography. Principles and examples of algorithms.
2. Asymmetric cryptography. Principles and examples of algorithms.
3. Distribution of keys using the principles of quantum mechanics.
4. Secure communication using SSL/TLS, IPsec, and VPN technology and protocols.
5. Wireless security - WiFi, Bluetooth, ZigBee and mobile networks.
6. Firewall - basic division, network and transport layer filtering methods, application inspection, IP tables.
7. Hash functions – principles of the safe hash function, use in practice, possible safety weaknesses.
8. Public Key Infrastructure (PKI) - key distribution options - DH algorithm, centralized and decentralized trust policy (CA, PGP), X.509 certificates, digital signature.
9. Intrusive detection and protection systems - function principles, deployment in network topology, differences in the use of IDS and IPS, examples of implementation.
10. Secure Shell - transport and authentication protocol SSH, versions, usage, examples of implementation.
11. Penetration testing - the principle and purpose of penetration tests, examples of tools and systems.

12. Cryptography, principles and examples of historical ciphers. Steganography.
13. Multimedia content security protocols - SRTP and ZRTP.
14. SIP protocol and its security - TLS and DTLS.
15. Handling of video and audio content, content mixing, manipulation of SIP signalling (registration, redirection and deliberate ending of sessions).
16. Honeypots used in multimedia sessions – fundamentals of the honeypot functions, basic methods of attack and anomaly detection, examples of implementation.
17. WebRTC and WebSockets from a multimedia security point of view - signalling and media transfer methods, key distribution methods, ISO/OSI layers in WebRTC.
18. Scanning and monitoring in IP telephony - the principle of detecting IP telephony devices, scanning methods and their detection.
19. Denial of service attacks in IP telephony - DoS methods, function principles and countermeasure options.
20. Man in the Middle in multimedia sessions - creation and deployment of the Man in the Middle attack, methods and risks of the signal and media capturing, MitM detection and defense.
21. Steganography in IP telephony - principles of the steganographic methods in signaling and media protocols, usage in the real environment, methods of detection.
22. Social attacks in VoIP - Spam in the IP telephony - principles, methods, utilization, Wangiri - principles, methods, utilization.
23. SIP and RTP traffic generators - principles, methods and examples of the deployment, creation of the templates, implementations.
24. Authentication in the SIP protocol - SIP protocol requests and responses with enabled authentication, authentication methods, authentication fields and creation of the control chain.

Last update 30.10.2023