Task 6 p 17

1. Antivirus software is a type of security software.

2. Antivirus software can run on various devices, including smartphones, tablets, personal computers (PCs), USB flash drives, servers, and Macs.

3. Antivirus software identifies malware through methods such as scanning for known virus signatures and heuristic analysis.

4. The process of searching for malware is called scanning or performing a virus scan.

5. The two techniques to look for a virus are:

- Searching for known virus signatures: This involves comparing files against a database of known virus signatures to identify malware.

- Heuristic analysis: This technique involves analyzing the behavior of files and programs to detect suspicious activities that may indicate the presence of malware.

6. A virus signature is a unique series of instructions or code segment that is part of a malware exploit. These signatures are discovered by security experts who examine the code of malware programs. When identified, virus signatures are added to a database of virus definitions used by antivirus software to detect and eliminate malware.

Task 7

1. True

2. False - Antivirus software is available for both personal computers and smartphones.

3. True

4. True

5. False - Antivirus software can examine various aspects of program code, including its behavior, not just its length.

6. False - A virus signature is a section of program code with a unique series of instructions, not a common one.

7. False - Virus signatures are discovered by security experts who examine the code of malware programs.

8. False - When virus signatures are discovered, they are added to a database of virus definitions, not deleted.

Task 2 p 19

The first definition appears to be more aligned with legal terminology and considerations. It focuses on the unlawfulness of damaging critical infrastructure and causing interruption or alteration of operations, which would typically be analyzed by a legal expert in terms of its implications for laws and regulations regarding cyberattacks.

The second definition seems to be more technical and related to the capabilities and effects of cyber weapons. It discusses the use of computer code to threaten or cause harm to structures, systems, or living beings, which would typically be analyzed by a security or technical expert.

Similarities:

1. Both definitions refer to the use of computer instructions or code.

2. They both mention causing harm or damage to systems or entities.

Differences:

1. The first definition emphasizes unlawfulness and damage to critical infrastructure, focusing more on legal aspects.

2. The second definition focuses on the intent and effects of cyber weapons, highlighting their potential to cause physical, functional, or mental harm, which is more technical in nature.

Task 3

1. Cyberspace is the virtual world created by information and communication technology, characterized by the absence of physical boundaries.

2. Illegal activities committed in cyberspace include espionage, theft of technology, financial fraud, and the spread of malware through means such as viruses, rootkits, and malware.

3. Cyber weapons can be classified according to four parameters:

- Precision: The capability to target specific objectives and reduce collateral damages.

- Intrusion: The level of penetration inside the target system.

- Visibility: The capability to remain undetected while operating.

- Ease of implementation: The resources needed to develop the specific cyber weapon.

4. Cyber weapons are attractive due to several factors:

- Complementarity with conventional military strikes, enhancing offensive operations.

- Efficiency and cost-effectiveness compared to traditional warfare.

- Speed of execution, as attacks can be carried out instantaneously.

- Difficulty in detection during the preparation and development phases.

5. Cyber weapons often target critical infrastructure and vital systems such as national defense systems, hospitals, water supplies, transportation control systems, air traffic controls, electricity grids, communication networks, and financial institutions.

6. The most dangerous effects of the use of cyber weapons include:

- Unpredictable diffusion, as cyberspace has no boundaries, leading to unintended consequences and collateral damage.

- Possibility of a "boomerang effect" where the attacker's systems are also affected.

- Potential for reverse engineering of cyber weapons by malicious actors, leading to the development of new cyber threats that are difficult to mitigate.