### **1 Digital security basics.**

Digital security is a critical aspect of information technology, as it involves protecting digital information and IT assets from both internal and external threats. This includes implementing strategies for prevention, detection, and response to these threats through security policies, software tools, and IT services. It’s essential for businesses of all sizes and industries to maintain strong security measures to prevent system compromises or data breaches.

Physical security is concerned with safeguarding personnel, hardware, software, networks, and data from potential harm, such as natural disasters, intrusions, or theft. For example, an attacker might use a USB device to steal sensitive data or introduce malware into systems.

Information security, or Infosec, covers a wide range of strategies for managing the processes, tools, and policies designed to protect both digital and non-digital information assets. This includes application security, which focuses on protecting applications from threats that could exploit vulnerabilities in the source code.

In summary, digital security encompasses various measures and strategies aimed at ensuring the integrity, confidentiality, and availability of information in the complex cyber environment of today. It’s a comprehensive approach that requires constant vigilance and adaptation to new threats.

### **2 Computer protection and maintenance.**

In the realm of computer protection and maintenance, it’s crucial to safeguard your computer from power surges. These sudden increases in electrical energy can cause significant damage to your computer’s circuit board and other electrical components. One of the ways to protect your computer from these surges is by using a surge suppressor. This device prevents the surge from reaching your computer when plugged into it, instead of directly into a wall outlet.

During thunderstorms, it’s advisable to take additional precautions. You should shut down your computer, turn off all peripheral devices, and unplug them from wall outlets. This includes any cables connected to your modem. This practice helps to prevent any potential damage from lightning-induced surges.

Another device that plays a crucial role in computer protection is an Uninterrupted Power Supply, or UPS. A UPS provides two main benefits. Firstly, it offers surge protection, similar to a surge suppressor. Secondly, it provides battery backup power during a power outage. This feature is particularly beneficial as it allows you to save any ongoing work and properly shut down your computer, preventing any data loss or damage to the system.

So, in essence, computer protection and maintenance involve a combination of practices and devices, such as surge suppressors and UPS, to ensure the longevity and optimal performance of your computer. These measures help to protect against electrical issues and maintain the health of your computer’s components.

### **3 Types of password attacks.**

In the digital world, password attacks are a significant threat to personal data security. One common form of attack is known as password hacking, where unauthorized individuals gain access to personal data illegally, often equated to identity theft. Hackers can easily discover passwords that are written down or stored insecurely.

There are several methods hackers use to carry out password attacks:

* Brute Force Attack: This involves using password-cracking software that tries every possible combination of letters, numbers, and symbols until the correct password is found. It’s a methodical approach that can take days to crack some passwords due to the sheer number of combinations.
* Sniffing: This technique is about monitoring and capturing data packets as they pass through a network. While network administrators use sniffers to monitor and troubleshoot network traffic, attackers use them to capture sensitive information, including passwords.
* Dictionary Attack: In this case, hackers use a dictionary of common passwords and phrases to guess your password. It’s a step above brute force attacks in terms of efficiency but relies on people using simple and common passwords.
* Key Logging: This is a more insidious method where a software secretly records a user’s keystrokes, including their passwords, and sends this information to the hacker.

These methods highlight the importance of strong, unique passwords and the need for vigilance in protecting personal information in an increasingly connected world. It’s a reminder that password security is a critical component of overall digital security.

### **4 Password security, authentication.**

Password security and authentication are vital components of digital security. A password manager, sometimes referred to as a keychain, is a tool designed to keep track of all your passwords so you don’t have to remember them. These managers can also autofill forms with stored addresses and credit card information, making online transactions more convenient.

Moreover, password managers can generate strong, random passwords composed of letters, numbers, and symbols, enhancing the security of your accounts. They often feature a strength meter that indicates the security level of your passwords, which is particularly useful if you prefer to create your own passwords rather than using the ones generated by the manager.

In addition to passwords, there are other forms of authentication like user IDs, PINs (personal identification numbers), and biometrics, which include facial features or fingerprints. Two-factor authentication protocols add an extra layer of security by requiring a second form of verification, such as a retinal pattern or a physical token, ensuring that only legitimate users gain access.

In our information age, where everyday activities like making online purchases, logging into Windows, or accessing wireless networks are commonplace, the importance of robust password security and reliable authentication methods cannot be overstated. They are the first line of defense in protecting our digital lives.

### **5 Malware, types, ways to be infected.**

Malware, which stands for malicious software, is a term that encompasses various types of harmful software designed to damage, disrupt, or gain unauthorized access to computer systems. Let’s talk about some common types of malwares and how they can infect your system:

* Viruses are notorious for their ability to replicate themselves and spread to other computers, often hitching a ride on an email attachment or through downloads.
* Trojan Horses masquerade as legitimate software, but once installed, they perform malicious activities behind the scenes.
* Worms are self-replicating malware that spread across networks by exploiting vulnerabilities, requiring no human interaction to propagate.
* Bots are automated processes that interact with network services, which can be used for malicious purposes.
* Spyware is designed to secretly collect information about users without their consent.
* Keyloggers record every keystroke made on a computer, capturing sensitive data such as passwords and credit card numbers.
* Adware bombards your screen with unwanted advertisements, typically within a web browser.
* Ransomware holds your files hostage by encrypting them and demanding payment for the decryption key.
* Rootkits allow attackers to remotely control a computer system without detection.

You can become infected with malware through various means, such as downloading attachments from unknown emails, visiting malicious websites, downloading pirated software, or failing to regularly update your software, which leaves vulnerabilities open to exploitation. It’s crucial to stay vigilant and use reputable security software to protect your computer from these threats. Remember, the best defense is a good offense, and in the case of malware, that means being proactive about your digital security.

### **6 Practices to avoid computer infection.**

To keep your computer safe from infections, it’s important to adopt certain practices.

Firstly, install security software like antivirus and anti-malware programs, and ensure they are always up to date. Regular updates are crucial as they often include patches for newly discovered vulnerabilities.

Secondly, update your operating system and other software. Developers release updates not just for new features, but also to fix security holes. Keeping your software current reduces the risk of infection.

Thirdly, be cautious with email attachments and links. Don’t open attachments or click on links from unknown or untrusted sources. These can often be disguised as legitimate but may contain malware.

Additionally, avoid clicking on pop-up ads and steer clear of suspicious websites. Pop-ups can be deceptive and lead to malicious sites or downloads, and some websites are known to host malware that can infect your system.

Lastly, disable the option to hide extensions for known file types in Windows. This helps you identify potentially harmful files before opening them, as some malware may masquerade as a harmless file type.

By following these practices, you can significantly reduce the risk of your computer becoming infected with malware. Always stay vigilant and informed about the latest security threats and how to counteract them. Remember, prevention is better than cure when it comes to computer security.

### **7 Antivirus software, techniques.**

Antivirus software is an essential defense mechanism for computers and devices, protecting against malware threats. It operates by scanning your system for malicious programs and uses a variety of techniques to detect and remove them. Here are some key techniques used by antivirus software:

* Virus Signatures: Antivirus programs maintain a database of known malware signatures—unique identifiers for each type of malware. When scanning, the software compares files against this database to find matches.
* Heuristic Analysis: This technique involves examining the behavior of programs to identify suspicious activities that may indicate malware. It’s particularly useful for detecting new or unknown threats that do not match any known signatures.
* Real-Time Scanning: Antivirus software often runs in the background, checking files as they are accessed or downloaded to prevent malware from infecting the system in the first place.
* Regular Updates: To stay effective, antivirus software must be updated regularly with the latest malware definitions and detection algorithms.

By employing these techniques, antivirus software helps to keep your digital environment secure. It’s important to choose a reputable antivirus solution and keep it updated to protect against the ever-evolving landscape of cyber threats. Remember, staying vigilant and informed is key to maintaining your cybersecurity.

### **8 Cyberwarfare attacks, cyber weapon.**

Cyberwarfare attacks:

Изображение выглядит как текст, Шрифт, белый, снимок экрана

Автоматически созданное описание

1. **Espionage**: This involves unauthorized access to confidential information. It’s like digital spying where attackers covertly gather sensitive data.
2. **Sabotage**: These attacks aim at the destruction or disruption of systems. The intent is to cause harm by damaging or disabling the target system or network.
3. **Denial-of-service (DoS) Attacks**: These attacks overwhelm systems making them unavailable. The goal is to overload the network or servers with unnecessary requests to deny service to legitimate users.
4. **Electrical Power Grid Attacks**: These attacks target electrical power grids with the aim to disrupt power supply. It can cause significant damage given our reliance on electricity for most services.
5. **Propaganda Attacks**: These attacks involve the spread of misleading or false information. The aim is to manipulate public opinion or obscure the truth.
6. **Economic Disruption**: These attacks target financial systems causing disruptions in economic activities. It can involve manipulating financial data, causing outages in financial services, etc.
7. **Surprise Attacks**: These are unexpected attacks that catch the target unprepared, causing significant damage. The sudden nature of these attacks makes them particularly effective.

Cyber weapon:

Cyber weapons are a modern form of weaponry used in the digital realm of cyberspace. Unlike traditional weapons, cyber weapons consist of software and processes designed to infiltrate, disrupt, or damage computer systems and networks. They play a significant role in cyber warfare and cyber terrorism, where they can be deployed to target critical infrastructure, steal sensitive information, or spread disinformation.

These weapons are particularly dangerous because they can be deployed stealthily, often remaining undetected until it’s too late. The targets of cyber weapons are not limited to military installations; they can include civilian facilities like hospitals, water supplies, and traffic control systems, making them a national security concern.

One of the most challenging aspects of cyber weapons is their detection and mitigation. Due to the virtual nature of cyberspace and the sophistication of these weapons, it can be incredibly difficult to identify and defend against them. This makes cybersecurity measures and awareness crucial in the modern age, as the threat of cyber-attacks continues to grow.

### **9 Social Engineering, state of the issue.**

Social engineering is a significant concern in the realm of cybersecurity. It involves the psychological manipulation of people to obtain confidential information or induce them to perform certain actions that compromise security. This deceptive practice exploits human vulnerabilities, such as the tendency to trust others or the desire to be helpful, making it a potent tool for scammers and hackers.

Here are some key points about social engineering:

* Human Psychology: It leverages human emotions and behaviors to trick individuals into divulging sensitive information or granting access to restricted areas.
* Common Tactics: These include phishing, pretexting, baiting, and tailgating, where attackers pose as trusted entities or create scenarios that prompt victims to act against their best interests.
* Rising Threat: With increasing digital connectivity, social engineering attacks have become more sophisticated and frequent, targeting both individuals and organizations.
* Prevention Measures: Education and awareness are crucial. People should be trained to recognize the signs of social engineering and encouraged to verify identities and requests before responding.

To combat social engineering, it’s essential to foster a culture of skepticism and caution when dealing with unsolicited requests, whether they come via email, phone, or in person. Implementing strict verification processes and promoting cybersecurity best practices can help mitigate the risks associated with these types of attacks.

### **10 Methods of social engineering.**

Social engineering is a deceptive practice where attackers use human interaction to obtain or compromise information about an organization or its computer systems. Here are some common methods used in social engineering:

* Phishing: Attackers send fraudulent emails resembling those from reputable sources to trick individuals into providing sensitive data.
* Pretexting: The attacker creates a fabricated scenario to gain the victim’s trust and gather personal information.
* Baiting: Similar to phishing, baiting involves offering something enticing to lure victims into a trap that steals their personal information or infects their systems with malware.
* Quid Pro Quo: Attackers offer a benefit in exchange for information. This benefit could be a service or a gift.
* Tailgating: An attacker seeks entry to restricted areas by following closely behind a legitimate employee.
* Shoulder Surfing: Direct observation techniques, such as looking over someone’s shoulder to get passwords or other sensitive information.

These methods exploit the natural human tendency to trust and can be very effective. It’s important to be aware of these tactics and to approach unsolicited requests for information with skepticism. Always verify the identity of the person you are communicating with and never give out personal information unless you are sure of the person’s authority and the legitimacy of the request.

### **11 Protection techniques against phishing, vishing, smishing.**

To protect against phishing, vishing, and smishing, it’s important to be vigilant and informed. Here are some techniques to safeguard yourself:

* Phishing: Always verify the authenticity of emails before clicking on links or downloading attachments. Look for signs of legitimacy, such as the sender’s email address and the language used in the email. Use email filters and security software to detect and block suspicious emails.
* Vishing: Be cautious when receiving unsolicited phone calls asking for personal information. Verify the caller’s identity by contacting the organization they claim to represent through official channels.
* Smishing: Treat text messages with the same skepticism as emails. Don’t click on links or provide information in response to text messages from unknown sources. Instead, contact the purported sender using a verified phone number.

Additionally, regularly update your security software, use multi-factor authentication where possible, and educate yourself about the latest social engineering tactics. By staying alert and cautious, you can significantly reduce the risk of falling victim to these types of attacks.

### **12 Encryption, its types, usage, importance.**

Encryption is a fundamental security measure that transforms readable data, known as plain text, into a coded form called cipher text. This process ensures that only authorized parties can access the original information. Here’s an overview of encryption, its types, usage, and importance:

Types of Encryptions:

* Symmetric Encryption: Uses a single key for both encryption and decryption. It’s efficient for large volumes of data but requires secure key management.
* Asymmetric Encryption: Employs a pair of keys, public and private. The public key encrypts data, while the private key decrypts it, facilitating secure communication between parties.

Usage:

* Data Protection: Encrypts sensitive information to prevent unauthorized access.
* Secure Communication: Ensures that messages remain confidential during transmission.
* Authentication: Verifies the identity of users and the integrity of transmitted data.

Importance:

* Privacy: Protects personal and confidential information from unauthorized access.
* Security: Shields against data breaches and cyber threats.
* Compliance: Meets regulatory requirements for data protection.

In addition to these points, encryption is also crucial for securing online transactions, protecting intellectual property, and maintaining the confidentiality of communications across various industries. Its role in safeguarding digital assets is more critical than ever in our increasingly connected world.