МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний авіаційний університет

Факультет аеронавігації, електроніки та телекомунікацій

Кафедра авіаційної англійської мови

МОДУЛЬНА КОНТРОЛЬНА РОБОТА

З дисципліни

«Англійська мова для професійного спілкування»

Галузь знань: 15 Автоматизація та приладобудування
Спеціальність: 151 Автоматизація та комп'ютерно-інтегровані технології
Освітньо-професійна програма:
Комп'ютеризовані системи управління та автоматика

Module 1

Name……
Group……
Date……

1. **Fill in the gaps with the following words:**

1). Online banking offers …..to monitor …..
   a) PINs, identity theft;
   b) accounts alerts, ball pay;
   c) electronic statements, accounts activity.

2)……software improves hard drive performance.
   a) CD-R;
   b) CD-RW;
   c) RAID.

3). A device for connecting an MP3 player to a computer.
   a) ACC;
   b) bitrate;
   c) decode.

4). A device that scans see-through objects.
   a) transparency adapter;
   b) digital camera;
   c) laser printer.

5). An online environment.
   a) Avatar;
   b) virtual world;
   c) link.

6). ……helps narrow the search.

a) Boolean operator;
b) Media;
c) License restriction.

7). Webpage with personal or identifying information.

a) Profile;
b) Forum;
c) link.

8). A feature that lets electronic message leave or listen to an electronic message.

a) Voicemail;
b) call waiting;
c) text massage

9). Online banks have a(n) ……and a(n) to secure transaction.

a) SSI connection, site key;
b) PIN, electronic statement;
c) account alert, bill pay.

2. Give it a name:

1. ……. is a person who breaks into a computer system. The reasons can be many: installing malware, stealing or destroying data, disrupting service, and more. It can also be done for ethical reasons, such as trying to find software vulnerabilities so they can be fixed.

2. …….. is a set of cybersecurity strategies that prevents unauthorized access to organizational assets such as computers, networks, and data. It maintains the integrity and confidentiality of sensitive information, blocking the access of sophisticated hackers.

3. …….is a set of technologies, products, and techniques that are designed to stop sensitive information from leaving an organization. It can end up in the wrong hands whether it's sent through email or instant messaging, website forms, file transfers, or other means. Its strategies must include solutions that monitor for, detect, and block the unauthorized flow of information.

4. ……..is a crucial component of next-generation solutions. It continues to evolve and adapt. For this reason, it can be extremely difficult to detect at the perimeter of the network. While threat intelligence can identify more threats, your network will still be challenged with new, never-seen-before malware. Some of this ware can have timers and other stealthy attributes that disguise malicious behavior until it has entered the network.

5. …….. raises the strength of all of these solutions. World-class threat intelligence transforms these technologies from good to great. Network protection and visibility increases an organization's ability to stop threats. All of this, however, assumes an organization can determine if a file is malicious or safe. This is unlikely. Most threats are unknown to the network. It can alert your network if an unknown threat has been deemed malicious somewhere else on the globe.

3. **Mach the items from the two groups (A and B):**

A) Current, World Wide, e-mail, surfing, download, web, computer.

B) Screen, the net, events, information, sites, Web, message.

4. **Read the text. Choose from the sentences (A-E) the one that best fits each gap (1-5) to complete the text.**

A). Devices that may be secured by this type of security include cell phones, tablets, laptops, and desktop computers.

B). This type of security can help secure the usage of software-as-a-service (SaaS) applications and the public cloud.

C). This type of security is necessary to prevent a hacker from accessing data inside the network.

D). This added layer of security involves evaluating the code of an app.

E). These protections are designed to monitor incoming internet traffic for malware as well as unwanted traffic.

Types of IT security

Network security is used to prevent unauthorized or malicious users from getting inside your network. This ensures that usability, reliability, and integrity are uncompromised. 1)…….It also prevents them from negatively affecting your users' ability to access or use the network. Network security has become increasingly challenging as businesses increase the number of endpoints and migrate services to public cloud.

Internet security involves the protection of information that is sent and received in browsers, as well as network security involving web-based applications. 2)……..This protection may come in the form of firewalls, antimalware, and antispyware.

Endpoint securite provides protection at the device level. 3)……..Endpoint security will prevent your devices from accessing malicious networks that may be a threat to your organization. Advance malware protection and device management software are examples of endpoint security.

Cloud security. Applications, data, and identities are moving to the cloud, meaning users are connecting directly to the Internet and are not protected by the traditional security stack. 4). ……A cloud-access security broker (CASB), secure Internet gateway (SIG), and cloud-based unified threat management (UTM) can be used for cloud security.

Application security are specifically coded at the time of their creation to be as secure as possible, to help ensure they are not vulnerable to attacks.

5)……It includes identification of the vulnerabilities that may exist within the software.

5. Fill in *a(an)* and the where necessary.

Inside a computer, there are five main components, the Motherboard, the Central Processing Unit, Random Access Memory, Storage, and Power Supply. Without these five parts, you simply don't have 1)….. computer. The Motherboard, sometimes referred to as the Mainboard or simply MoBo, is 2) …… large printed circuit board. Its job is to connect all the devices on your computer to each other. Everything inside and outside of the PC connects to the motherboard, and through 3)……. Motherboard, to every other component. When you plug in 4) ……. mouse or keyboard, attach your screen, speakers/headphones or a microphone, or any USB device such as 5)…… printer, flash drive, external hard drive, they're all plugging into the motherboard. The Central Processing Unit, sometimes called 6)……. CPU or just Processor, is 7)……brains of the machine. Virtually everything you do on your computer runs through the CPU. The CPU is mounted onto the motherboard in 8)….. socket. Most of the time it's simply plugged in, but occasionally it's soldered into place. Looking carefully at the lines (wires) on a motherboard, you'll see that most of them lead to the processor, either directly or indirectly. It's the CPU that actually runs all 9)…… programs on your computer, including Windows itself. Inside a PC, everything is connected to the CPU through the motherboard.

Розробник: доктор пед. наук, професор кафедри Оксана ПЕРШУКОВА