**Unit VIII. Computer Viruses**

*VOCABULARY STUDY*

**Word List**

***Nouns and noun phrases***

Vulnerability ─ уязвимость, незащищенность; partition table ─ таблица разбиения дисков; decline ─ уменьшение; removal ─ удаление; header ─ верхний колонтитул; footer ─ нижний колонтитул; Multipartite virus ─ комбинированный вирус; registry ─ реестр;

***Adjectives and collocations***

malware program ─ вредоносная программа; self-replicating ─ самовоспроизводящийся; bootable ─ загрузочный; overall ─ итоговый; overwrite virus ─ вирус в режиме наложения записи; conventional ─ обычный; high-end software ─ профессиональное, высокопроизводительное ПО; unsolicited ─ нежелательный; non-replicating ─ не воспроизводящийся; legitimate ─ законный; remote access ─ удаленный доступ;

***Verbs, Adverbs***

Intentionally ─ намеренно; trigger ─ запускать; inject ─ вводить; breach ─ находить брешь; propagate ─ распространять; embed ─ встраивать; robust ─ устойчивый к сбоям; shut down ─ завершать работу; inherently ─ внутренне.

**I. Match the words with the definitions below.**

*Malicious 5, malware 7, damage 1, identity 2, threat 11, to pretend 9, to score 3, to spread 12, scam 6, to disguise 4, to replicate 14, to prevent 13, to encrypt 10, firewall 8.*

1. physical harm that is done to an object

2. who you are, your name, date of birth, etc.

3. to cause great fear, frighten

4. to make something unrecognizable by changing its appearance

5. intended to do harm

6. an illegal trick with the purpose of getting money from people

7. malicious software

8. a computer system or program that automatically blocks an unauthorized access to a computer when it is connected to the Internet

9. to claim that something is true, when it is not

10. to convert data into a special code to prevent unauthorized access

11. a danger that something unpleasant might happen to people

12. to gradually reach a larger area or more people

13. to stop something from happening

14. to make an exact copy, reproduce

**II. Using a dictionary add as many words as possible into the table.**

|  |  |  |
| --- | --- | --- |
| ***Verbs***  1. to boot  2. part  3. to infect  4. restore  5. locate  6. to encrypt  7. extend | ***Adjectives***  bootable  partial  infective  restored  local  encrypted  extensive | ***Nouns***  boot  partition  infection  restoration  location  encryption  extension |

**III. Choose the words with similar meaning from the two groups and arrange them in pairs.**

A. Partition, root, overload, encryption, remote, malware, inject, web scripting.

B. Virus, access, a code, directory, program, table, key, the network.

Partition table, root directory, overload network, encryption key, remote access, malware program, inject a code, web scripting Virus

**IV. Match the words with a similar meaning. Check any unknown words in a dictionary.**

1. To delete; 2. Malicious; 3. Charges; 4. To replicate; 5. Scam; 6. Identity; 7. Secure; 8. Damage;

a. Expenses, costs; b. To duplicate; c. Harm; d. To remove; e. Safe; f. Harmful; g. Fraud; h. Personal information.

1d2c3a4b5g6h7e8f

**V. Match the words. Check that you know the meanings of the phrases. Then complete the sentences below.**

*1) commit; 2) unauthorized; 3) phishing; 4) antivirus; 5) security; 6) self-replicating; 7) built-in; 8) verify;*

*a) program b) firewalls c) access d) email e) information f) crimes g) software h) warning.*

1. Virus is a *self-replicating program*  that interferes with a computer’s hardware or operating system. 2. Some computers come with security software. Windows 7 and Mac OS X already have *built-in software*. 3. *Antivirus firewalls*  can protect you from infected email attachments, Internet worms, and fake websites. 4. Cybercriminals *verify crimes* by stealing people’s money or their identity data. 5. *Phishing email* is disguised to look like official communications from a legitimate website. 6. Once installed, spyware programs can have *unauthorized access*  to user’s activities – such as Internet surfing habits and browser activity. 7. If you *commit* i*nformation* about your identity on a fake website, scammers can use these details to withdraw money from your bank account. 8. When you visit a malicious site your browser will display a red *security* *warning* message.

**VI. Translate the following sentences into English.**

1. Существует ряд Интернет угроз, с которыми мы можем столкнуться в сети: кража личных данных, шпионское программное обеспечение, фальшивые антивирусы и другие вредоносные программы. 2. Хорошее антивирусное программное обеспечение должно предлагать защиту в режиме реального времени. 3. – Что может заблокировать несанкционированный доступ к компьютеру из сети? 4. Однажды установив антивирусное программное обеспечение, вам необходимо обновлять его регулярно. 5. – Я не уверен, какой антивирус подойдет для моего компьютера. Что вы можете мне посоветовать? – Попробуйте загрузить бесплатную пробную версию вот этого программного обеспечения. Оно предоставляет защиту высокого уровня без замедления работы вашего устройства. 6. – Тебе бы лучше сделать резервные копии твоих файлов в сети, другими словами, в облаке. – Какая разница? – Когда ты хранишь информацию в облаке, она сохраняется на сервере в Интернете. Ты всегда можешь иметь доступ к своим файлам, даже если компьютер поврежден. 7. Вам не следует открывать почтовые приложения, полученные от незнакомых людей или нажимать на ссылку, содержащуюся в письме. Иначе вы можете стать жертвой кибермошенничества. 8. – Мне помочь тебе с программой по шифрованию? – Да, пожалуйста. Я не могу полностью разобраться в ней.

Перевод:

1. There are a number of Internet threats that we may encounter online: identity theft, spyware, fake antiviruses and other malicious programs. 2. Good antivirus software should offer real-time protection. 3. – What can block unauthorized access to the computer from the network? 4. Once you have installed antivirus software, you need to update it regularly. 5. – I am not sure which antivirus is suitable for my computer. What can you advise me? – Try downloading a free trial version of this software. It provides high-level protection without slowing down your device. 6. – You'd better make backups of your files on the network, in other words, in the cloud. – What's the difference? – When you store information in the cloud, it is stored on a server on the Internet. You can always have access to your files, even if the computer is damaged. 7. You should not open mail applications received from strangers or click on the link contained in the letter. Otherwise, you may become a victim of cyberbullying. 8. – Can I help you with the encryption program? – Yes, please. I can't quite figure it out.

*A. TEXT STUDY*

**I. Read the text and answer the following questions.**

1. Why do most programs catch viruses?

Most systems catch viruses due to program bugs, the vulnerability of operating systems, and poor security practices.

2. What criteria can computer viruses be categorized according to?

types of computer viruses that can be categorized according to their origin, spreading capabilities, storage location, files they infect and destructive nature

3. Enlist the types of viruses and characterize them briefly.

*1. Boot Sector Virus* infects the storage device’s master boot record (MBR).

*2. Direct Action Virus* This very quickly get into the main memory, infects all programs/files/folder defined in Autoexec.bat path and then deletes itself. It can also destroy the data present in hard disk or USB attached to the computer.

*3. Overwrite Virus* delete the data (partially or completely) and replace the old code with their own. They replace the file content without changing its size.

*4. Web Scripting Virus* breaches web browser security and allows attackers to inject client-side scripting into the web page. They propagate quite faster than other conventional viruses.

*5. Directory Virus.*

*6. Polymorphic Virus.*

*7. Memory Resident Virus.*

*8. Macro Virus*

*9. Companion Virus.*

*10. Multipartite virus.*

*11. FAT Virus*

*12. Trojan Horse.*

*13.Computer worms*

4. What can each type of virus affect? Give examples.

*1. Boot Sector Virus* can affect the operation of the hard drive

*2. Direct Action Virus* can affect all programs/files/folder. Itdoesn’t delete system files but alter the system’s overall performance. It can affect all .exe and .com file extension.

*3. Overwrite Virus* simply delete the data (partially or completely) and replace the old code with their own.

*4. Web Scripting Virus* can affect web browser

*5. Directory Virus.*

*6. Polymorphic Virus.*

*7. Memory Resident Virus.*

*8. Macro Virus*

*9. Companion Virus.*

*10. Multipartite virus.*

*11. FAT Virus*

*12. Trojan Horse.*

*13.Computer worms*

5. What are the protection measures against each type of virus?

*1.* To protect against the *Boot Sector Virus*, make sure that the disk you are using is write-protected. Do not start/restart the computer with unknown external disks connected.

*2. Direct Action Virus* Use antivirus scanner. Direct action virus is easy to detect and all infected files can be restored completely.

*3. Overwrite Virus* is to delete all the infected files, so it’s better to keep your antivirus program updated, especially if you are using Windows.

*4. Web Scripting Virus* Use malicious software removal tool in Windows, disable scripts, use cookie security or install real-time protection software for the web browser.

*5. Directory Virus.*

*6. Polymorphic Virus.*

*7. Memory Resident Virus.*

*8. Macro Virus*

*9. Companion Virus.*

*10. Multipartite virus.*

*11. FAT Virus*

*12. Trojan Horse.*

*13.Computer worms*

6. What are logic bombs?

Logic Bombs. They are not a virus but inherently malicious like worms and viruses. It is a piece of code intentionally inserted (hidden) into a software tool. This code is executed after certain criteria are met.

**TEXT A. Computer Viruses**

A computer virus is a malware program that is written intentionally to gain access to a computer without its owner’s permission. These kinds of programs are primarily written to steal or destroy computer data. Most systems catch viruses due to program bugs, the vulnerability of operating systems, and poor security practices.

There are different types of computer viruses that can be categorized according to their origin, spreading capabilities, storage location, files they infect and destructive nature. Do you know the first-ever computer virus (named Creeper) was an experimental self-replicating program written by Bob Thomas at BBN Technologies in 1971?

*1. Boot Sector Virus.* Boot Sector virus infects the storage device’s master boot record (MBR). Any media, whether it is bootable or not can trigger this virus. These viruses inject their code to hard disk’s partition table. It then gets into the main memory once the computer restarts. Booting problems, unstable system performance and inability to locate hard disk are common issues that may arise after getting infected. However, it has become rare since the decline in floppy disks. Modern operating systems come with an inbuilt boot sector safeguard. The virus can affect any file after getting into the main memory. Examples: Form, Disk Killer, Stone virus, Polyboot.B. Protection: Make sure that the disk you are using is write-protected. Do not start/restart the computer with unknown external disks connected.

*2. Direct Action Virus.* This virus quickly gets into the main memory, infects all programs/files/folder defined in Autoexec.bat path and then deletes itself. It can also destroy the data present in hard disk or USB attached to the computer. While these viruses are found in hard disk’s root directory, they are capable of changing location on every execution. In most cases, they don’t delete system files but alter the system’s overall performance. It can affect all .exe and .com file extension. Example: VCL.428, created by the Virus Construction Laboratory. Protection: Use antivirus scanner. Direct action virus is easy to detect and all infected files can be restored completely.

*3. Overwrite Virus.* Overwrite viruses are very dangerous. They have affected a wide range of operating system including Windows, DOS, Macintosh, and Linux. They simply delete the data (partially or completely) and replace the old code with their own. They replace the file content without changing its size. It is easy to detect as the original program stops working. Once the file gets infected, it can’t be restored and you will end up losing all data. It can affect any file. Examples: Grog.377, Grog.202/456, Way, Loveletter. Protection: The only way to get rid of this virus is to delete all the infected files, so it’s better to keep your antivirus program updated, especially if you are using Windows.

*4. Web Scripting Virus.* A web scripting virus breaches web browser security and allows attackers to inject client-side scripting into the web page. They propagate quite faster than other conventional viruses. It is used to attack large sites like social networking, user review or email. It has the potential to send a large amount of spam, fraud activity, and damage files on sever. It can affect any web page by injecting hidden code in header, footer or root access file. Examples: DDos, JS.fornight. Protection: Use malicious software removal tool in Windows, disable scripts, use cookie security or install real-time protection software for the web browser.

*5. Directory Virus.* Directory Virus (also known as Cluster virus) infects the file by changing the DOS directory information. In this case, DOS points to the virus code rather than pointing to the original program. When you run a program, DOS first loads and executes the virus code before running the actual program code. It becomes very difficult to locate the original file after getting infected. It can affect: The entire program in the directory. Example: Dir-2. Protection: Install the antivirus to relocate the misplaced files.

*6. Polymorphic Virus.* The polymorphic virus encodes themselves using different encryption keys and algorithms each time they infect a program or create a copy of itself. Because of different encryption keys, it becomes very difficult for the antivirus software to find them. In other words, it is a self-encrypted virus which is designed to avoid detection by scanners. It can affect any file. Examples: Whale, Simile, SMEG engine, 1260. Protection: Install advanced, high-end antivirus software.

*7. Memory Resident Virus.* These viruses live in primary memory (RAM) and get activated whenever you switch on the computer. They affect all files currently running on the desktop. Basically, it allocates memory, blocks original scripts, and runs its own code when any program is executed. It can affect any file running on PC and files that are being copied or renamed. Examples: Randex, Meve, CMJ. Protection: Install strong antivirus software.

*8. Macro Virus.* There are a few software such as a word processor that allows a macro program to embed in documents. This virus is written in the macro language, so it may run automatically when the document is opened and it can easily spread to other files too. It depends on the application rather than the operating system. They are generally hidden in documents that are more likely shared via email. It can affect: .mdb, .PPS, .Doc, .XLs files. Examples: Bablas, Concept and Melissa virus. Protection: Disable macros and don’t open emails from unknown sources. Alternatively, you can install modern antivirus software that can detect macro virus easily.

*9. Companion Virus.* Companion Viruses were more popular during the MS-DOS era. Unlike traditional viruses, they do not modify the existing file. It creates a copy of a file with a different extension (usually .com) which runs in parallel with the actual program. For example, if there is a file named abc.exe, this virus will create another hidden file named abc.com. And when the system calls a file ‘abc’, the .com (higher priority extension) runs before the .exe extension. It can perform malicious steps such as deleting the original files. Can affect: All .exe files. Examples: Stator, Terrax.1096. Protection: Can be easily detected because of the presence of additional .com file. Install reliable antivirus software and avoid downloading attachments of unsolicited emails.

*10. Multipartite virus.* The Multipartite virus infects and spreads in multiple ways depending on the operating system. They usually stay in memory and infect the hard disk. Once it gets into the system, it infects all drives by altering applications’ content. You will soon start noticing performance lag and low virtual memory available for user applications. It can affect: Files and boot sector. Examples: Ghostball, Invader. Protection: Clean boot sector and entire disk before reloading the data. Do not open attachments from a non-trusted internet source and install quality antivirus software.

*11. FAT Virus.* FAT stands for file allocation table which is a section of storage disk that is used to store information, such as the location of all files, total storage capacity, available space, used space etc. A FAT virus alters the index and makes it impossible for the computer to allocate the file. It is powerful enough to force you to format the whole disk. It can affect any file. Example: The link virus. Protection: Avoid downloading files from non-trusted sources, especially those identified as “attack site” by browser or search engine. Use robust antivirus software. Other malware that are not Virus but are equally dangerous.

*12. Trojan Horse.* Trojan Horse (or Trojan) is a non-replicating type of malware that looks legitimate. Users are typically tricked into loading and executing it on the system. It can destroy/modify all the files, crash the computer, modify the registry, and is strong enough to give hackers remote access to your PC. Examples: ProRat, ZeroAccess, Beast, Netbus, Zeus. Protection: Use reliable high-end antivirus software and update it regularly.

*13.Computer worms.* Worm is a standalone malware program that replicates itself in order to spread to other computers. It relies on networks (mostly emails) and security holes to travel from one system to another. Unlike viruses, it overloads the network by replicating or sending too much data, forcing the hosts to shut down the server. Example: Code red, ILOVEYOU, Morris, Nimda, Sober, WANK. Protection: Use antivirus and anti-spyware software.

Logic Bombs. They are not a virus but inherently malicious like worms and viruses. It is a piece of code intentionally inserted (hidden) into a software tool. This code is executed after certain criteria are met.

**II. Comprehension Check. State whether the statements are true or false. Correct if necessary.**

1. A malware program is written intentionally to steal money from bank account without its owner’s permission.

2. Booting problems have become rare since the decline in floppy disks.

3. In most cases, boot sector viruses don’t delete system files but alter the system’s overall performance.

4. Once the file gets infected by overwrite viruses, it can’t be restored and you will end up losing all data.

5. Logic Bombs are used to attack large sites like social networking, user review or email.

6. When you run a program, DOS first loads and executes the virus code before running the actual program code.

7. Memory resident virus is a self-encrypted virus which is designed to avoid detection by scanners.

8. Companion viruses are generally hidden in documents that are more likely shared via email.

9. Companion viruses can be easily detected because of the presence of additional .com file.

10. FAT virus stays in memory and infect the hard disk.

11. Trojan Horse can destroy/modify all the files, crash the computer, modify the registry, and is strong enough to give hackers remote access to your PC.

**III.** **Do a brief quiz below to test your knowledge about Internet Security.**

**Internet Security Quiz**

1. Viruses, worms, and Trojans are all examples of \_\_\_.

a) pets that can be seen in a zoo;

b) phishing;

c) malware;

d) scareware.

2. What is malware?

a) hardware that controls a computer without the user’s knowledge;

b) faulty software;

c) hardware that detects and removes viruses from a computer;

d) software created to cause harm to a computer system or data.

3. What is a virus?

a) a program that makes user feel unwell;

b) a program which replicates itself and spreads to other computers via attachments;

c) a program that monitors user’s activities;

d) a program that stops a computer from working.

4. Malware can be downloaded through \_\_\_.

a) spam emails;

b) infected computers;

c) unsafe websites;

d) all of the above.

5. What is spyware?

a) malware that harms your computer by deleting or altering files and stopping programs from running;

b) malware that tricks you into thinking it is software you need to buy;

c) malware that collects information from a computer and sends it to cybercriminals;

d) malware that pretends to be a trusted file.

6. What is the purpose of phishing?

a) controlling computer without user’s knowledge;

b) sending a program that replicates itself and spreads to other computers via attachments;

c) sending a malicious link disguised as a security warning;

d) sending an email that is designed to trick the user into giving away personal information.

7. What should be used to remove malware from a computer?

a) a filter;

b) antivirus software;

c) encryption;

d) a firewall.

8. How can one safeguard against phishing?

a) Install a firewall.

b) Don’t believe everything you read on the Net.

c) Make backup copies of your files regularly.

d) Don’t follow a link from the email you don’t trust.

9. What is the purpose of a firewall?

a) to detect viruses on a system and prevent them from attacking it and spreading;

b) to prevent unauthorized connections coming into and out of a network;

c) to prevent from illegal copying and distribution of copyrighted software, information, music, etc.;

d) to prevent a hacker from logging on to the computer.

10. Which of the following is a simple way to stay safe online?

a) Don’t open email attachments from unknown people.

b) Run and update antivirus programs.

c) Don’t give out personal information.

d) All of the above.

**IV. Rephrase the sentences using modal verbs.**

*Example: It’s a good idea to back up the files. You’d better back up the files.*

1. I advise you to transfer files via a secure connection.

You'd better transfer files via a secure connection

2. Do not download unknown files.

You should not download unknown files.

3. Students must be on time for all their classes.

Students are obliged to be on time for all their classes.

4. It isn’t a good thing to open email attachments from people you don’t know.

you shouldn't open email attachments from people you don’t know.

5. I advise you to turn on a firewall.

You'd better turn on a firewall.

6. You don’t need to contact technical support. Jim has already called them.

You should not contact technical support. Jim has already called them.

7. It’s necessary to use mail encryption to send sensitive data.

You must use mail encryption to send sensitive data.

8. It is the best thing to keep your antivirus software updated.

You'd better keep your antivirus software updated.

9. It’s a good idea to set user access levels on your laptop.

You'd better set user access levels on your laptop

10. You are not allowed to make any changes to the system.

You can’t make any changes to the system.

11. Don’t use a public Wi-Fi for shopping and banking.

You should not use a public Wi-Fi for shopping and banking.

12. It’s necessary for you to create a strong password to stop criminals from accessing your private information.

You'd better create a strong password to stop criminals from accessing your private information.

**V. Correct the mistakes.**

1. I have to e-mail some urgent letters. 2. You can’t ~~to~~ access the network. 3. You ~~don~~’t mustn’t be late for the exam. 4. Sasha couldn’t ~~can’t~~ remove malware from his computer yesterday. 5. ~~Do I could use your laptop?~~ Could I use your laptop?

*B. TEXT STUDY*

**I. Read the text and answer the following questions.**

1.Prove that Google Chrome is the most popular web browser in the world.

2. Why do you need to clear your cache?

3. What are extensions used for?

4. What are malware and adware extensions?

5. What way does a top-performing web browser benefit business?

**How to Make Google Chrome Superfast**

Google Chrome is the most popular web browser in the world with over 2 billion installs, 1 billion users, and 53% share of the market. Its speed is one of its most notable advantages over other existing browsers, as well as one of the reasons why it’s preferred by most netizens. But even the fastest browser experiences some performance drops from time to time. If your Chrome has slowed down, here are simple hacks to get it back into tip-top shape in no time.

*Clear your browsing data.* Chrome stores a cached copy of a website you visit, so it can load the page faster when you visit it again. It also keeps a database of your browsing history and cookies for the same purpose. As you visit more and more websites, these pieces of data accumulate in Chrome and can slow the browser down.

Thankfully, the solution to this is easy: clear your cache. To do this, simply access your browsing history by entering chrome://history on your address bar. From the left panel, select Clear browsing data. Choose which data will be deleted by clicking on the checkboxes of all items you want to delete, like cached images or cookies. You can also select the time range that will be affected by the deletion. You can delete your history for the past hour, the last 24 hours, the last 7 days, the last 4 weeks, or from the beginning of time. Once you’ve selected the files you want to delete and their corresponding time range, click Clear data.

*Disable extensions.* Extensions are downloadable programs from the Chrome Web Store that you can add to your browser to give it more functionality and a personalized touch. For example, you can add an extension that blocks ads, one that shortens URLs, or one that shows you your most important tasks of the day. While these extensions are useful, they can slow Chrome down when there are too many installed at once.

Most extensions will show on Chrome’s address bar, and you can quickly uninstall them by right-clicking on their icons and selecting Remove from Chrome. You can also manage all extensions by typing chrome://extensions on your browser and hitting Enter. From there, you’ll find a list of all the extensions you have (even those you don’t remember installing). Simply scroll through the list and click Remove to delete the extensions you don’t need.

*Remove ads and malware.* Sometimes, Chrome slows down because of malware or adware extensions. Extra toolbars, recurring pop-up ads, and web pages redirecting to other addresses are clear indications of these. Google once had a downloadable app developed for Chrome that scans and removes unwanted programs called the Clean Up Tool. In 2018, Google discontinued that app and made malware scanning even easier. Just go to chrome://settings/cleanup on your browser, and click on Find to find and remove harmful software on your computer.

A top-performing web browser benefits your business in many ways, including upping employees’ productivity and speeding up communication processes. It’s therefore critical that yours is fast and reliable. If your web browser is performing poorly or takes forever to load a page, don’t hesitate to get in touch with us so we can identify and fix the problem right away.

**II. Comprehension Check. State whether the statements are true or false. Correct if necessary.**

1. Google Chrome performance is one of its most notable advantages over other existing browsers.

2. As you visit more and more websites, these pieces of data accumulate in Chrome and can accelerate the browser up.

3. Once you’ve selected the files you can restore the information easily.

4. Extensions are reloadable programs from the Chrome Web Store.

5. Most extensions will show on Chrome’s address bar.

6. One can quickly install extensions by right-clicking on their icons and selecting Update from Chrome.

7. Chrome may slow down because of malware or adware extensions.

8. If your web browser is performing poorly, ask your provider for help.

**III. Fill in many / much, a lot of / lots of / few / little / a few / a little.**

**Sometimes more than one option is suitable.**

1. There are \_\_\_ various operating systems for you to choose from.

2. There were not \_\_\_ convenient means of communication 20 years ago.

3. Is there \_\_\_ difference between HDMI cables and HDMI Ethernet switch?

4. There are only \_\_\_ applications supported by this OS.

5. There is very \_\_\_ battery charge left. Bring up the charge adapter please.

6. You had better install a good anti-virus system because there \_\_\_ phishing attacks on the Internet now.

7. There is too \_\_\_ free space on my memory stick to copy this software. I need to use a different one.

8. There were quite \_\_\_ adequate ideas in his speech regarding our project.

9. There used to be very \_\_\_ service at this company and it was very bad.

10. There are \_\_\_ useful laboratories equipped with cutting-edge computing machines at the BSTU.

11. There were \_\_\_ good gadgets in the shop, that quite \_\_\_ customers wanted to buy.

**IV. Fill in some, any, no and their compounds in the sentences. Sometimes more than one option is suitable.**

1. There is \_\_\_ important about our research I must tell you.

2. There is \_\_\_ need to reinstall Windows, as it has a high performance.

3. Do you know if \_\_\_ attends courses on programming?

4. \_\_\_ special was added to a new version of this smartphone.

5. Are there \_\_\_ commentaries on this application usage?

6. Can you provide users with \_\_\_ more Internet security?

7. All people will benefit from \_\_\_ you do at your job.

8. You can use \_\_\_ authorized version of Windows, they are all quite reliable.

9. There is \_\_\_ wrong with the operating system of this computer. You must repair it immediately.

10. There are not \_\_\_ chances for \_\_\_ hackers’ attacks with this antivirus system.

11. Can you give us \_\_\_ more time to finish our presentation?

**V. Put the verbs in brackets in the correct (Active or Passive) form**

**using the Present Simple or Future Simple Tense.**

Google Spreadsheet (be) a free web best application similar to Microsoft itself. You (create) and (edit) spreadsheets for all kinds of projects including contact lists. To get started, the create button (click) and a spreadsheet (choose). First, we (have) a toolbar, where different shortcuts (access). The print command, undo and redo options (include) as well as the self-format and font size (control) by the user. To view even more options the menus above the toolbar (use). Thus, you (give) access to many additional features. You (navigate) back to Google drive to title up you spreadsheet so that it is easier to find a file again in the future. There (be) no save button, because Google spreadsheet (use) the auto save feature, which automatically (save) your file any time you (make) a change. Finally, you (find) a comments button and a share button. You (allow) to collaborate with other Google Drive users and you quickly (manage) your sharing options. Each spreadsheet (consist) of cells, columns and rows for your data. A cell (be) the interaction of a row and a column. There (be) also the formula bar where text, formulas and functions for a specific cell (enter). At the very bottom of the window additional sheets (add) to your spreadsheet by clicking a plus button.

**VI. Speak about computer viruses and internet security measures using key words, phrases and the topic sentences.**