ФКФН,

2 курс,
группа КБ-11, 2 подгруппа

Тексты и задания для самостоятельной работы задолжников:

Text 1 (Unit 6)

Exercise 1. Memorize the words:

to spread – v.распространять(ся)
n. распространение
to threaten – угрожать > в текст
harmful – вредный
to halt – останавливать(ся) > в текст
loose – a. свободный, широкий; небрежный > в текст
v. освобождать, развязывать
to hide – прятать, скрывать > в текст
malicious – злобный; предумышленный
to be aware – знать, сознавать; отдавать себе отчет
to constitute – составлять
to distinguish – проводить различие, различать
distinction – разница, различие > в текст
to replicate – копировать
replication – копирование > в текст
replicant – копия > в текст
to intend – предназначать; подразумевать
intentional – преднамеренный, умышленный
in turn – в свою очередь > в текст
to pretend – притворяться, делать вид > в текст
to destroy – разрушать, уничтожать > в текст
to fulfil – выполнять, осуществлять > в текст
to cause – причинять, вызывать, быть причиной
damage – v. повреждать, портить, наносить ущерб
n. вред, повреждение, ущерб
due to – благодаря > в текст
entirely – полностью > в текст
to launch – запускать > в текст
to propagate – размножать(ся); распространять(ся) > в текст
rarely – редко > в текст
deletion – стирание, удаление > в текст
subtle – коварный, запутанный > в текст
self-contained – замкнутый, полный > в текст

Exercise 2. Read and translate the text.

Computer Viruses

What are computer viruses and why should we worry about them? They are spreading faster than they are being stopped, and even the least harmful of viruses could be life-threatening. For example, in the context of a hospital life-support system, a virus, that "simply" stops a computer and displays a message until a key is pressed, could be fatal. Further, those who create viruses can not halt their spread, even if they wanted to.

Many people use the term "virus" loosely to cover any sort of program that tries to hide its possibly malicious function and/or tries to spread onto as many computers as possible, though some of these programs may more correctly be called "worms" or "Trojan Horses". Computer viruses are actually a special case of something known as "malicious logic" or "malware". It can be important to understand the distinctions between viruses and other forms of malware.

The best definition we have been able to come up with is the following 4-part one:

1) A virus is a program that is able to replicate, that is create (possibly modified) copies of itself.
2) The replication is intentional, not just a side-effect.
3) At least some of replicants in turn are also viruses by the same definition.
4) A virus has to attach itself to a "host", in the sense that execution of the host implies execution of the virus.

Part 1 of the definition distinguishes viruses from non-replicating malware, such as Trojans, ANSI bombs and logic Bombs.

Part 2 distinguishes between viruses and programs such as DISKCOPY.COM that can replicate.

Part 3 of the definition is needed to exclude certain intended viruses, that attempt to replicate, but fail – they simply do not qualify as "real" viruses.

Part 4 is necessary to distinguish between viruses and worms, which do not require a host.

A Trojan Horse is a non-replicating program that pretends to do something useful (or at least interesting), but when it is run, it may have some harmful effect, like scrambling your FAT (File Allocation Table) or formatting the hard disk.

Viruses and Trojans may contain a "time-bomb", intended to destroy programs or data on a specific date or when some condition has been fulfilled. A time bomb is often designed to be harmful, maybe doing something like formatting the hard disk. Sometimes it is relatively harmless, perhaps slowing the computer down every Friday or making a ball bounce around the screen. However, there is really no such thing as a harmless virus. Even if a virus has been intended to cause no damage, it may do so in certain cases, often due to the incompetence of the virus writer.

A computer WORM is a self-contained program (or set of programs), that is able to spread functional copies of itself or its segments to other computer systems (usually via network connections). Unlike viruses, worms do not need to attach themselves to a host program. There are two types of worms-host computer worms and network worms. Host computer worms are entirely contained in the computer they run on and use network connections only to copy themselves to other computers. Host computer worms where the original terminates itself after launching a copy on another host (so there is only one copy of the worm running somewhere on the network at any given moment), are sometimes called “rabbits”. Network worms consist of multiple parts (called “segments”), each running on different machines (and possibly performing different actions) and using the network for several communication purposes. Propagating a segment from one machine to another is only one of those purposes. Network worms that have one main segment which coordinates the work of the other segments are sometimes called “octopuses”.

A virus may be modified, either by the original author or someone else, so that a more harmful version of it appears. It is also possible that the modification produces a less harmful virus, but that has only rarely happened.

The damage caused by a virus may consist of the deletion of data or programs, maybe even reformatting of the hard disk, but more subtle damage is also possible. Some viruses may modify data or introduce typing errors into text. Other viruses may have no intentional effects other than just replicating.

(to be continued)

Text 2 (Unit 7)

Exercise 1. Memorize words and word combinations:

to be concerned about – беспокоиться о (по поводу…) > в текст
to contaminate – заражать, загрязнять > в текст
to boot – 1. n. начальная загрузка
2. v. загружать(ся)
bootstrap area – область начальной загрузки > в текст
to replace smth with – заменять, подменять что-либо, чем-либо > в текст
partition – 1. n. раздел; > в текст
2. v. выделять разделы
to overwrite – переписывать > в текст
to attempt – пытаться, стараться
target – цель, мишень, задание, план > в текст
to distribute – распространять > в текст
to pose a threat – представлять угрозу > в текст
a dropper program – программа – переносчик > в текст
to inoculate against – делать прививку, проводить вакцинацию против > в текст
victim – жертва > в текст

Exercise 2. Read and translate the text

Virus types

The kind of viruses any user has to be most concerned about are Boot Record, DOS, macro and Master Boot Record infections.

Boot Record viruses usually infect systems through a contaminated boot floppy. These viruses operate by moving the original (uninfected) system boot record to a location unknown to the operating system. They then replace the original boot record with an infected one. Typically, Boot Record viruses move the uninfected system boot record to the end of the boot partition. The virus overwrites any data present in this area.

There are two types of typical DOS virus programs. Direct-action viruses attempt to modify specifically targeted programs or files present on a system when the virus executes. Memory resident viruses place themselves in RAM, where they attempt to modify any program that runs.

Macro viruses are malicious routines written in an application program's macro language. The first identified macro virus was written in WordBasic and distributed as part of a normal Word for Windows document file. Any program that supports automatic execution of macros contained within data files poses a potential virus threat.

Master Boot Record (MBR) viruses are programs that infect the bootstrap area of a bootable floppy disk or hard drive. On DOS systems, they become resident in memory when the operating system loads. An MBR virus is usually caused by booting a system from an infected floppy disk or by a so-called “dropper” program that places the virus on the hard drive's boot sector.

Most viruses try to recognize existing infections, so they do not infect what has already been infected. This makes it possible to inoculate against specific viruses, by making the “victim“ appear to be infected. However, this method is useless as a general defense, as it is not possible to inoculate the same program against multiple viruses.

In general, viruses are just programs – rather unusual programs perhaps, but written just like any other program. It does not take a genius to write one – any average assembly language programmer can easily do it. Fortunately, few of them do.

Text 3 (Unit 8)

Exercise 1. Memorize words and word combinations:

embedded – встроенный; вложенный > в текст
to seize – схватывать, захватывать > в текст
viral – вирусный > в текст
disease – болезнь, заболевание > в текст
deliberate – 1. намеренный; 2. обдуманный > в текст
to inflict – наносить, причинять > в текст

to taunt – насмехаться, говорить колкости > в текст

conventional – 1. обычный, общепринятый, традиционный; 2. условный > в текст

to trigger – запускать, инициировать > в текст

slightly – слегка > в текст

to alter – менять(ся); изменять(ся) > в текст

discreetly – осмотрительно, благоразумно > в текст

backup – резервная копия

failure – сбой, отказ, выход из строя > в текст

sufficient – достаточный > в текст

to survive – выжить, пережить > в текст

behaviour (ам. behavior) – поведение > в текст

to indicate – указывать, показывать > в текст

to remove – удалять, устранять

to detect – обнаруживать

to surface – всплывать (зд. проявляться) > в текст

a set period – установленный срок > в текст

lie dormant – бездействовать (dormant - бездействующий) > в текст

strictly speaking – строго говоря > в текст

extremely rarely – чрезвычайно редко > в текст

by accident – случайно > в текст

so as not to – так, чтобы не > в текст

shrink-wrapped – в фирменной упаковке > в текст

“stealth” virus – “скрытый” вирус > в текст

apart from – помимо, кроме > в текст

the only – единственный > в текст

to interfere with – мешать (кому-л., чему-л.) > в текст

to protect … from – защищать, предохранять … от > в текст

protection against – защита от > в текст

Exercise 2. Read and translate the text.

Most viruses known today were originally implanted in existing systems software or applications software on a PC disk. The virus may be appended to an existing program or embedded in the program’s code.

When the program is executed the virus seizes control of the computer and tries to replicate itself by copying the viral code to a non-infected program on the same or another disk. After reproduction which is carried out relatively quickly so as not to draw the attention of the user, the virus transfers control to the host program.

Following a period of reproduction which varies from virus to virus, the disease usually will surface by making some powerful and deliberate demonstration of its presence. This demonstration ranges from a benign- if annoying- display of a screen message, to the erasing of a hard disk without warning. While inflicting damage, viruses have been known to taunt users with messages like “We hope you’ve enjoyed our program”, “The time is my”, etc.

Newer better-designed viruses discreetly clone themselves and place copies on all available disk media, especially floppy-disks – the conventional path for transferring programs and data between PCs.

Some viruses are programmed to do no harmful actions for a set period. Depending on how they were designed, they could be programmed to reproduce or lie dormant. Others are triggered by a specific date, still others link activation to random intervals or a predefined cycle. For example, a spread-sheet virus may slightly alter the results of a recalculate operation every hundredth time it is executed.

Once a virus is identified and removed from the system, one of the major challenges is to prevent reinfection.

Apart from using anti-virus program, there are several ways to protect your computer from viruses:

Rule number one is: MAKE BACKUPS!!! Keep good backups (more than one) of everything you do not want to lose. This will not only protect you from serious damage caused by viruses, but is also necessary in the case of a serious hardware failure.

Never boot a computer with a hard disk from a diskette because that is the only way the hard disk could become infected with a boot sector virus. (Well, strictly speaking, it can happen if you run a “dropper” program too, but that happens extremely rarely).

If your BIOS allows you to change the boot sequence to “C: A:”, do it. This will give you very good protection against boot sector virus infections.

Should you, by accident, have left a non-bootable diskette in drive A: when you turn the computer on, the message

Not a system disk.

may appear. If the diskette was infected with a virus, it will now be active, but may not have infected the hard disk yet (Most boot sector viruses will do it right away, however). If this happens, remove the diskette from the A: drive and turn the computer off (or press the reset button). It is important to note that pressing Ctrl-Alt-Del is not sufficient, as a few viruses can survive that.

If the computer has no hard disk, but is booted from a diskette, you should always use the same diskette, and keep it write-protected.

Keep all diskettes write-protected unless you need to write to them. When you obtain new software on a diskette, write-protect the diskette before you make a backup copy of it. If it is not possible to make a backup of the diskette, because of copy-protection, it is not recommended to use the software.

Be really careful regarding your sources of software. In general, shrink-wrapped commercial software should be “clean”, but there have been a few documented cases of infected commercial software.

Check all new software for infection before you run it for the first time. It is even advisable to use a couple of scanners from different manufacturers, as no single scanner is able to detect all viruses.

Look out for any “unusual” behaviour on your computer, like:

Does it take longer than usually to load programs?

Do unusual error messages appear?
Does the memory size seem to have decreased?
Do the disk lights stay on longer than they used to?
Do files just disappear?

Anything like this might indicate a virus infection.

If your computer is infected with a virus – DON'T PANIC! Sometimes a badly thought out attempt to remove a virus will do much more damage than the virus could have done. If you are not sure what to do, leave your computer turned off until you find someone to remove the virus for you.

Finally, remember that some viruses may interfere with the disinfection operation if they are active in memory at that time, so before attempting to disinfect you MUST boot the computer from a CLEAN system diskette.

It is also a good idea to boot from a clean system diskette before scanning for viruses, as several "stealth" viruses are very difficult to detect if they are active in memory during virus scanning.

Text 4

Read, translate and retell the text:

COMBATING VIRUSES, WORMS AND TROJAN HORSES

1. Trojans, viruses or worms can make computers or a network unstable and in many cases, unusable. The first steps to protecting your computer are to ensure your operating system (OS) is up-to-date. This is essential if you are running a Microsoft Windows OS. Secondly, you should have antivirus software installed on your system and ensure you download updates frequently to ensure your software has the latest fixes for new viruses, worms and Trojan horses. Additionally, you need to make sure your antivirus program has the capability to scan e-mail and files as they are downloaded from the Internet. This will help prevent malicious programs from even reaching your computer. You should also install a firewall.

2. A firewall is a system that prevents unauthorized use and access to your computer. A firewall can be either hardware or software. Hardware firewalls provide a strong degree of protection from most forms of attack coming from the outside world and can be purchased as a stand-alone product or in broadband routers. Unfortunately, when battling viruses, worms and Trojans, a hardware firewall may be less effective than a software firewall, as it could possibly ignore embedded worms in out-going e-mails and see this as regular network traffic.

3. For individual home users, the most popular firewall choice is a software firewall A good software firewall will protect your computer from outside attempts to control or gain access to your computer, and usually provides additional protection against the most common Trojan programs or e-mail worms. The downside (or disadvantage) to software firewalls is that they will only protect the computer they are installed on, not a network.

4. It is important to remember that on its own a firewall is not going to rid you of your computer virus problems, but when used in conjunction with regular

operating system updates and a good anti-virus scanning software, it will add some extra security and protection for your computer or network.

Text 5

Read, translate and retell the text:

NETWORK SECURITY

1. Not long ago a new kind of worm, known as Storm, began to sweep through the Internet. It hasn't received much attention in the mainstream press, but it has given security professionals more than a few sleepless nights. Storm is far more sophisticated than previous worms, because it uses peer-to-peer technologies and other new techniques to avoid detection.

2. Storm methodically infiltrates computers with inactive code that could be used to damage the whole network of a company, creating opportunities for getting money illegally. And Storm's creators, whoever they are, continue to modify their dangerous product even as it already stands as a dark cloud poised over the Internet.

3. Network security software products on the market today offer only limited defence. They use firewalls, which simply block access to unauthorized users, and software patches, which can be created only after a worm or virus's unique bit pattern is decoded. By the time this-difficult process of hand coding *is* complete, the worm has had hours and hours to spread, mutate, or be modified by its creators.

4. A new kind of answers needed. Network security researchers are developing software that can rapidly detect a wide variety of intrusions from worms, viruses, and other attacks without the high rate of false alarms that outbreaks many conventional Internet security products. These new programs can detect any anomalous network behavior in seconds and block threats. This new generation of algorithms is based on concepts related to the thermodynamic concept of entropy. Often defined briefly as a measure of the disorder of a system, entropy as a cornerstone of thermodynamic theory goes back more than a century and a half. But as a construct of information theory it is only 60 years old, and its application to data communications began only in the last decade or so.