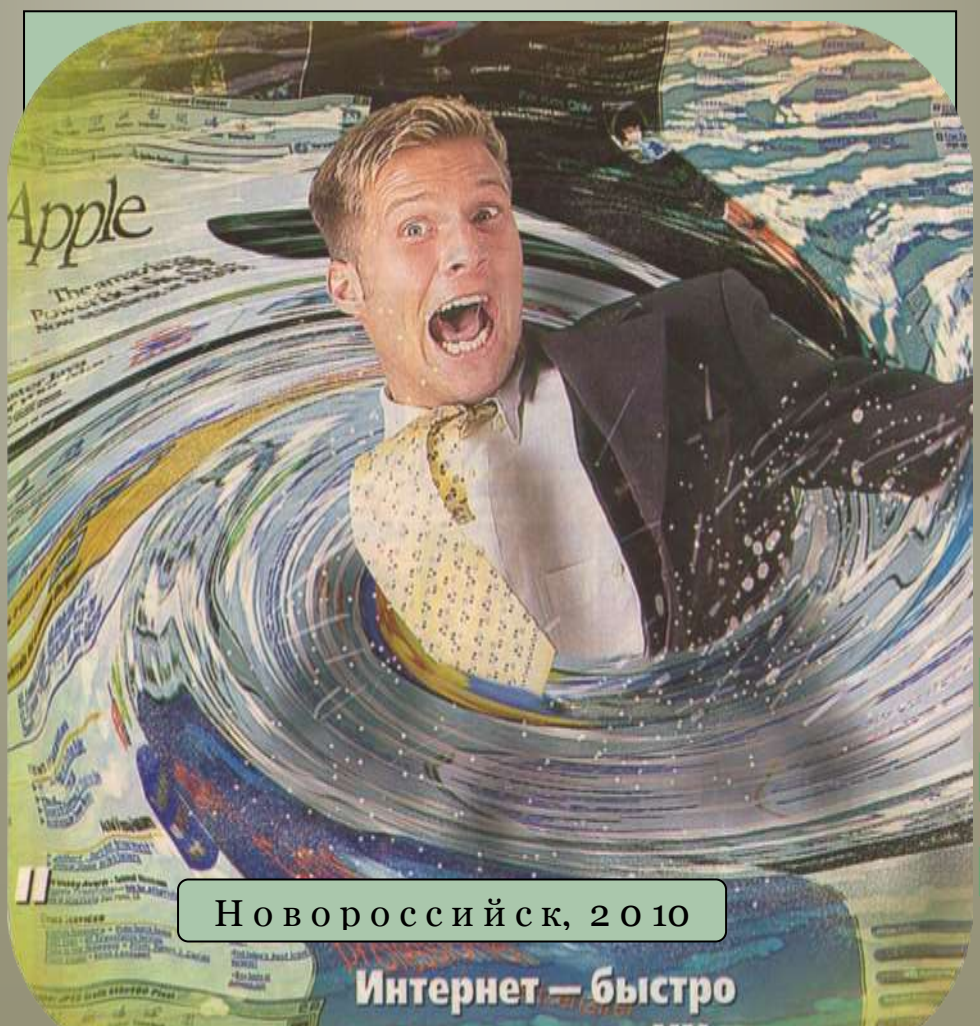
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«НОВОРОССИЙСКИЙ КОЛЛЕДЖ РАДИОЭЛЕКТРОННОГО ПРИБОРОСТРОЕНИЯ»

МЕТОДИЧЕСКАЯ РАЗРАБОТКА

по дисциплине «Иностранный язык»
(английский язык)
для студентов IV курса
специальности
«Программное обеспечение вычислительной техники и автоматизированных систем»

«Компьютерные вирусы. Вирусы и вакцины»



Новороссийск, 2010

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

«НОВОРОССИЙСКИЙ КОЛЛЕДЖ РАДИОЭЛЕКТРОННОГО ПРИБОРОСТРОЕНИЯ»

МЕТОДИЧЕСКАЯ РАЗРАБОТКА

по дисциплине «Иностранный язык» (английский язык)

по теме «Компьютерные вирусы. Вирусы и вакцины»

для студентов IV курса специальности «Программное обеспечение вычислительной техники и автоматизированных систем»

Новороссийск 2010

Одобрено

цикловой комиссией
филологических дисциплин
Председатель:

_____ С.П. Тихонова
«____» _____ 2010 г.

УТВЕРЖДАЮ

Зам. директора по УР

_____ Е. В. Заслонова
«___» _____2010 г.

Разработала: Марарь Марина Александровна – преподаватель НКРП

Рецензент: Тихонова Светлана Павловна – председатель ЦК филологических дисциплин

АННОТАЦИЯ

Настоящая учебно-методическая разработка «Компьютерные вирусы. Вирусы и вакцины» предназначена для работы студентов 4 курса специальности «Программное обеспечение вычислительной техники и автоматизированных систем». Взятые для разработки тексты (в основном, из учебного пособия «English for Computer Science Students»), составляют большую часть учебного материала, изучаемого студентами по данной теме; также студентам предлагаются тексты (в приложении) для более детальной отработки содержания материала, который рассчитан на I семестр (14 учебных занятий). Так как упомянутое пособие и подобранные мною тексты из различных источников по специальности предназначены для студентов 4 курса, поэтому считаю, что указанный материал с предлагаемыми последующими упражнениями соответствует уровню подготовки студентов.

Начиная работу, хочу отметить, что тексты профессионально направлены, и, естественно, без знаний и специальных предметов могут возникнуть языковые трудности и трудности перевода. Во избежание этих трудностей предусмотрена поэтапная работа с текстами, ряд упражнений и заданий для их последовательного разбора по частям, а также выявления сути и краткого изложения на изучаемом языке.

Учебно-методическая разработка включает в себя:

- тексты «The History of Computer Viruses», «What is a Computer Virus?», «File Viruses», «Computer Viruses», «Viruses and Vaccines»;
- список лексики, которую необходимо знать студентам и использовать в речи;
- устно-речевые задания;
- приложения, которые включают в себя аналогичные тексты по заданной теме.

Все послетекстовые задания составлены автором разработки, список лексики также подобран автором.

Применение данной разработки на практике помогает решить поставленные задачи, а именно:

- ✓ развивать навыки чтения текста и его понимание;
- ✓ использовать навык чтения изучающего и поискового характера;
- ✓ развивать монологическую речь;
- ✓ развивать логическое мышление студентов;
- ✓ закреплять грамматические навыки, полученные в процессе обучения.

Материал разработки рассчитан на среднего студента, а при надлежащем изучении доступен пониманию и мышлению каждого из студентов, находящемся на 4 курсе обучения в среднем профессиональном учебном заведении. Разработка соответствует установкам программы по английскому языку, а последовательность подобранных заданий имеет логическую направленность, соответствующую логике развития данной отрасли.

Преподаватель_____Марарь М.А.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Компьютерные вирусы. Что это такое и как с этим бороться? На эту тему уже написаны десятки книг и сотни статей, борьбой с компьютерными вирусами профессионально занимаются сотни (или даже тысячи) специалистов в десятках (а может быть, сотнях) компаний. Казалось бы, тема эта не настолько сложна и актуальна, чтобы стать объектом такого пристального внимания. Однако это не так. Компьютерные вирусы были и остаются одной из наиболее распространенных причин потери информации. Известны случаи, когда вирусы блокировали работу организаций и предприятий. Более того, несколько лет назад был зафиксирован случай, когда компьютерный вирус стал причиной гибели человека – в одном из госпиталей Нидерландов пациент получил летальную дозу морфия по той причине, что компьютер был заражен вирусом и выдавал неверную информацию. Несмотря на огромные усилия конкурирующих между собой антивирусных фирм, убытки, приносимые компьютерными вирусами, не падают и достигают астрономических величин в сотни миллионов долларов ежегодно. При этом следует отметить, что антивирусные программы и «железо» не дают полной гарантии защиты от вирусов. Примерно также плохо обстоят дела на другой стороне тандема «человек-компьютер». Как пользователи, так и профессионалы-программисты часто не имеют даже навыков «самообороны», а их представления о вирусе порой являются только поверхностными. Здесь очень важно знать одно, что – *обязательным свойством компьютерного вируса является возможность создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению.*

Данная работа рассматривает на английском языке само понятие ВИРУС, немного информации из его истории возникновения, типы / виды вирусов, дает представление о файловых вирусах, способах их обнаружения, удаления, и, если возможно, лечения. Помимо теоретической части, в разработке даны задания и упражнения на практику применения полученных знаний как на занятиях по спецпредметам, так и на уроках английского языка.

THE HISTORY OF COMPUTER VIRUSES

2 November, 1988, Robert Morris younger (Robert Morris), **graduate student** of informatics faculty of Cornwall University (USA) **infected** a great amount of computers, connected to Internet network. This network **unites** machines of university centres, private companies and governmental agents, including National Aeronautics Space Administration, as well as some military scientific centres and labs.

Network worm has struck 6200 machines that formed 7,3 % computers to network, and has shown, that UNIX **is not okay** too. Amongst damaged were NASA, LosAlamos National Lab, exploratory center VMS USA, California Technology Institute, and Wisconsin University (200 from 300 systems). **Spread on** networks ApraNet, MilNet, Science Internet, NSF Net it practically has **removed** these network from building. According to "Wall Street Journal", virus has **infiltrated** networks in Europe and Australia, where there were also registered events of blocking the computers.

Here are some **recalls** of the event participants:

Symptom: hundreds or thousands of jobs start running on a UNIX system bringing response to zero.

Systems attacked: UNIX systems, 4.3BSD UNIX & variants (e.g.: SUNs) any sendmail compiled with **debug** has this problem. This virus is spreading very quickly over the Milnet. Within the past 4 hours, it has hit more than 10 sites across the country, both Arpanet and Milnet sites. Well over 50 sites have been **hit**. Most of these are "major" sites and gateways.

Method: Someone has written a program that uses **a hole** in SMTP Sendmail **utility**. This utility can send a message into another program.

Apparently what the attacker did was this: he or she connected to sendmail (i.e., telnet **victim** machine 25), issued the appropriate debug command, and had a small program **compiled**. (We have it. **Big deal**.) This program took as an argument a host number, and copied two programs -one ending in *VAX.OS* and the other ending in *SunOS* - and tried to load and **execute** them. In those cases where the load and execution **succeeded**, the worm did two things (at least): **spawn** a lot of **shells** that did nothing but **clog** the process table and burn CPU cycles; look in two places - the password file and the internet services file - for other sites it could connect to (this is **hearsay**, but I don't doubt it for a minute). It used both individual host files (which it found using the password file), and any other remote hosts it could locate which it had a chance of connecting to. It may have done more; one of our machines had a changed super user password, but because of other factors we're not sure this worm did it.

All of *Vaxen* and some of *Suns* here were infected with the virus. The virus forks repeated copies of itself as it tries to spread itself, and the load **averages** on the infected machines **skyrocketed**. In fact, **it got to the point** that some of the machines ran out of **swap space** and **kernel** table entries, preventing login to even see what was going on!

The virus also "cleans" up after itself. If you **reboot** an infected machine (or it crashes), the directory is normally cleaned up on reboot. The other incriminating files were already deleted by the virus itself.

4 November the authors of the virus - Morris - come to FBI headquarters in Washington on his own. FBI has imposed a prohibition on all material relating to the Morris virus.

22 January, 1989, a court of jurors has **acknowledged** Morris **guilty**. If **denunciatory verdict** had been approved without modification, Morris would have been **sentenced to** 5 years of **prison** and 250 000 dollars of **fine**. However Morris' **attorney** Thomas Guidoboni immediately has **lodged a protest** and has directed all papers to the Circuit Court with the petition **to decline** the decision of court... Finally Morris was sentenced to 3 months of prisons and fine of 270 thousand dollars, but in addition Cornwall University **carried a heavy loss**, having excluded Morris from its members. Author then had to take part in liquidation of its own creation.

THE HISTORY OF COMPUTER VIRUSES

1. Mind new words from the Text:

1) **graduate student** – аспирант
2) **to infect** – заражать
3) **to unite** – соединять, объединять
4) **to be not okay** – быть не в порядке (о системе)
5) **spread on** – зд. распространившись на
6) **to remove** – удалять, уничтожать
7) **to infiltrate** – проникать, просачиваться
8) **recalls** – отзывы
9) **debug** – отладка программы
10) **hit** – зд. пораженный
11) **a hole** – дыра, отверстие
12) **utility** – обслуживающая программа
13) **apparently** – как видно, ясно, очевидно
14) **victim** – жертва
15) **to compile** – составлять
16) **Big deal**. – Хорошая сделка.
17) **to execute** – приводить в исполнение
18) **to succeed** – достигнуть, добиться
19) **spawn** – множественное размножение
20) **shell** – оболочка (пользовательский интерфейс)
21) **clog** – препятствие
22) **hearsay** – слух, сплетня
23) **to average** – достигать, проделывать в среднем
24) **to skyrocket** – быстро увеличиваться, расти (в размерах, о количеству, объёме)
25) **it got to the point** – он достигает цели
26) **to reboot** – перезагружать (компьютер)
27) **to acknowledge smb guilty** – признавать кого-л. виновным
28) **denunciatory verdict** – обвинительный приговор
29) **to be sentenced to prison and fine** – приговорить к тюрьме и штрафу
30) **attorney** – адвокат
31) **to lodge a protest** – подать протест
32) **to decline** – отклонить
33) **to carry a heavy loss** – понести тяжелые потерю

2. Define and write down the point of the text. Write what damage Robert Morrison caused to FBI headquarters in Washington, Cornwall University and other users.

3. Write out the Text all words which are connected with the word "virus". Translate them.

WHAT IS IT A COMPUTER VIRUS?

A computer virus is a computer program that can copy itself and **inflect** a computer without the permission or knowledge of the owner. The term "virus" is also commonly but **erroneously** used to refer to other types of **malware, adware, and spyware programs** that do not have the **reproductive ability**. A true virus can only spread from one computer to another (in some form of **executable code**) when its host is taken to the target computer; for instance, because a user sent it over a network or the Internet, or carried it on a removable medium such as a floppy disk, CD, DVD, or USB drive. Viruses can increase their chances of spreading to other computers by inflecting files on a network file system or a file system that is accessed by another computer. The term "computer virus" is sometimes used as a **catch-all phrase** to include all types of malware. Malware includes computer viruses, worms, Trojan horses, most root kits, spyware, dishonest adware, crime ware, and other **malicious** and unwanted software, including true viruses. Viruses are sometimes confused with computer worms and Trojan horses, which are technically different. A worm can **exploit** security **vulnerabilities** to spread itself to other computers without needing to be transferred as part of a host, and a Trojan horse is a program that appears harmless but has a hidden **agenda.** Worms and Trojans, like viruses, may **cause harm** to either a computer system's hosted data, functional performance, or networking throughput, when they are executed. Some viruses and other malware have symptoms noticeable to the computer user, but many are **surreptitious**. Most personal computers are now connected to the Internet and to local area networks, f**acilitating** the spread of malicious code. Today's viruses may also take advantage of network services such as the World Wide Web, E-mail, Instant Messaging, and file sharing systems to spread.

WHAT IS IT A COMPUTER VIRUS?

1. Mind new words from the Text:

1. **to inflect –** заражать, инфицировать

2. **erroneously –** неправильно, ошибочно

3. **agenda –** профиль, программа

4. **malware, adware, and spyware programs –** почтовые, вспомогательные и шпионские программы

5. **reproductive ability –** репродуктивная способность, способность воспроизводить

6. **executable code –** выполнимый, осуществимый код

7. **catch-all phrase –** всеохватывающая фраза

8. **malicious –** злостный, злоумышленный, вредный

9. **to exploit –** использовать, эксплуатировать

10. **vulnerabilities –** слабые места

11. **to** cause **harm –** причинять вред

11. **surreptitious –** потайной, тайный, подпольный

12. f**acilitating –** облегчать, помогать, способствовать

2. True or False?

1) A computer virus is a computer program that can copy itself and inflect a computer without the permission or knowledge of the owner.

2) A true virus cannot spread from one computer to another (without any form of executable code) when its host is taken to the target computer.

3) Viruses can increase their chances of spreading to other computers by inflecting files on a network file system or a file system that is accessed by another computer.

4) The term “computer virus” cannot be used as a catch-all phrase to include all types of malware.

5) Malware includes computer viruses, but doesn't deal with worms, Trojan horses, most root kits, spyware, dishonest adware, crime ware, and other **malicious** and unwanted software, including true viruses.

6) A worm can exploit security vulnerabilities to spread itself to other computers without needing to be transferred.

3. Put the proper words into sentences:

1. A true virus can only… one computer to another when its host is taken to the target computer; for instance, because a user sent it over a network or the Internet, or carried it on … such as a floppy disk, CD, DVD, or USB drive.

2. Viruses can … their … of spreading to other computers by inflecting files on …. or a file system that is accessed by another computer.

3. … are sometimes confused with computer worms and Trojan horses, which are technically different.

4. … is a program that appears harmless but has a hidden agenda.

5. Worms and Trojans, like viruses, may cause harm to either a computer system's hosted data, functional performance, or…, when they are executed.

6. Most … are now connected to the Internet and to local area networks, facilitating the spread of ….

Personal computers, spread from, increase… chances, networking throughput, a network file system, viruses, malicious code, a removable medium, a Trojan horse.

FILE VIRUSES

They write down the code in a body of an executed file. At start of the infected program the virus the first receives **management**, **searches for** the next **victim** and writes down in it the code, and then transfers control to the program so the user notices nothing. The method of **distribution** of file viruses is simple enough. Usually for infection something gets out interesting: the new game, **self-revealing archive** with the attractive name or the new version of the popular program. However, even if not to use programs of a doubtful origin, it is possible to catch through access to Internet or to it **similar** or **to** receive rather new version of a file virus - the macro command virus **extending** with documents of office **applications**, such as Word for Windows or Excel. Documents of office applications **comprise** not only the text and graphic representations, but also macros. The virus can change existing macros and to add new, introducing the body in a document file. For **preventive maintenance** of macro command viruses the anti-virus programs, capable to search for similar infections are necessary.

FILE VIRUSES

1. Mind new words from the Text:

1. **management -** администрирование
2. **to search for –** искать что-либо
3. **victim –** жертва
4. **distribution –** распределение
5. **self-revealing archive –** самообнаруживающийся, самопроявляющийся архив
6. **similar to –** похожий на
7. **to extend –** расширять(ся); удлинять(ся)
8. **application –** 1) использование, (практическое) применение 2) прикладная система, прикладная программа 3)приведение в действие.
9. **to comprise –** включать, охватывать

10. **preventive maintenance –** плановое техническое обслуживание и ремонт

2. Find in the text the English equivalents to:

Ищет следующую жертву, закодированный текущий файл, пораженная вирусом программа, способные находить похожие заражения, пользователь ничего не замечает, новая версия файлового вируса, включает графическое изображение, привлекательное название, вирус может менять существующие макрокоманды, метод распределения файловых вирусов.

3. Put the proper words into sentences:

1. The method of…. of file viruses is simple enough.

2. Even if not to use programs of …, it is possible to catch through … to Internet or to it similar or to receive rather new version of….

3. Documents of office … comprise not only the text and graphic representations, but also ….

4. For … of macro command viruses the anti-virus programs, capable to search for similar … are necessary.

Distribution, a doubtful origin, access, a file virus, applications, macros, preventive maintenance, infections.

4. True or False?

1) They write down the code in a body of an executed file.

2) Documents of office applications comprise only the text and not graphic representations, also macros.

3) Usually for infection something gets out interesting: the new game, self-revealing archive with the attractive name or the new version of the popular program.

4) Even if to use programs of a doubtful origin, it is possible to catch through access to Internet or to it similar or to receive rather new version of a file virus - the macro command virus extending with documents of office applications, such as Word for Windows or Excel.

COMPUTER VIRUSES

The Maltese Amoeba may sound like **a cartoon character**, but if it attacked your computer, you wouldn't be laughing. The Maltese Amoeba is a computer virus. It is a form of software which can "**infect**" your system and destroy your data. Making computer viruses is only one type of computer crime. Others include hacking (changing data in a computer without permission) and pirating (illegally copying software programs). Viruses are programs which are written **deliberately to damage** data. Viruses can **hide themselves** in a computer system. Some viruses are **fairly** harmless. They may flash a message on screen, such as *'Gotcha'! Bet you don't know how I crept in'*. The Yankee Doodle virus plays this American tune on the computer's small internal speaker every eight days at 5 p.m. Other has serious effects. They **attach** themselves to the operating system and can **wipe out** all your data or turn it into **gobbledygook**. When the Cascade virus attacks, all the letters in a file **fall into a heap** at the bottom of the screen. This look **spectacular** but it's hard to see the funny side when it's your document. Most viruses **remain dormant** until **activated** by something. For example, the Jerusalem B virus is activated every Friday the 13th and **erases** any file you try to load from your disk. The Michelangelo virus was programmed to become active on March 6th 1992, the 517th birthday of Michelangelo. It attacked computer systems throughout the world, turning data on hard disks into nonsense. Viruses are most commonly passed **via** disks but they can also spread through bulletin boards, local area networks, and email attachments. The best form of treatment is prevention. Use an antivirus program to check a floppy before using it. Always download email attachments onto a floppy and **check for** viruses. If you do catch a virus, there are antivirus programs **to hunt down and eradicate** the virus. The

problem is that around 150 new viruses appear every month and you must constantly **update** your **antivirus package to deal with** these new forms.

COMPUTER VIRUSES

1. Mind new words from the Text:

1. **a cartoon character** – мультипликационный персонаж

2. "i**nfect**" – поражать, инфицировать

3. **deliberately to damage** – намеренно, чтобы навредить

4. **to hide themselves** – скрываться, прятаться

5. **fairly** –зд. совсем

6. **to attach** – крепить; прикреплять; присоединять

7. **to wipe out** – стирать, уничтожать

8. **gobbledygook** – перлы (пренебрежительно!)

9. **to fall into a heap** – обрушиваться (в бездну, пучину)

10. **spectacular** - зрелищный, фееричный, эффектный

11. **to be activated** – быть приведенным в действие

12. **to erase** – стирать, уничтожать

13. **via** – через

14. **to check for** – проверять

15. **to hunt down and eradicate** – искать(разыскивать, гоняться за) и искоренять, вытравлять, ликвидировать, уничтожать

16. **to update antivirus package** – обновлять антивирусный пакет

17. **to deal with** – иметь дело с

18. **to remain dormant** – бездействовать

2. Find in the text the English equivalents to:

Если вирус напал на ваш компьютер, подобно мультперсонажу, Мальтийская Амёба, компьютерное преступление, поразить вашу систему и уничтожить информацию, изменение компьютерных данных без ведома кого-либо, пишутся намеренно, для того, чтобы навредить, могут прятаться в компьютерной системе, абсолютно безвредны, «Ба! Спорим, ты не знаешь, как я сюда проник?», другие имеют серьёзные последствия, могут уничтожить вашу информацию и превратиться в «перлы», буквы файла каскадом обрушиваются

вниз экрана, хоть и выглядит это зрелищным, но в этом мало приятного, если это ваш документ, некоторые вирусы бездействуют до тех пор, пока их не активировали, например, вирус активируется каждую пятницу 13го и удаляет любую инфо, которую вы пытаетесь загрузить с диска, другой вирус активируется в день Рождения Миккеланджелло, вирусы почти обычно проникают с диска, самое лучшее лечение – это предотвращение, если вы подхватили вирус – есть антивирусные программы, которые ищут и уничтожают вирус, около 150 вирусов появляются каждый месяц и вы должны постоянно обновлять антивирусную защиту.

3. To join the synonyms by pairs and translate them:

To attack, through, to pass, to creep in, to catch a virus, to emerge, to be transmitted, to find, to eradicate the virus, to remain dormant, to infect, to destroy, to fix, to assault, to hide themselves, to be inactive, to activate, to conceal, to see the funny side, via, to laugh, to erase, to hunt down, to damage, to appear, to wipe out, to make computer viruses, to attach themselves, to spread, to become active, to harm, to write a computer virus.

4. Put the proper words into sentences:

The Jerusalem B, disks, computer crime, to damage data, eradicate, update your antivirus package, the computer's small internal speaker, birthday of Michelangelo, antivirus program, the operating system.

---

1) Making computer viruses is only one type of…

2) Viruses are programs which are written deliberately….

3) The Yankee Doodle virus plays this American tune on … every eight days at 5 p.m. Other has serious effects.

4) They attach themselves to … and can wipe out all your data or turn it into gobbledygook.

5) … virus is activated every Friday the 13th and erases any file you try to load from your disk.

6) The Michelangelo virus was programmed to become active on March 6th 1992, the 517th ….

7) Viruses are most commonly passed via… but they can also spread through bulletin boards, local area networks, and email attachments.

8) Use an… to check a floppy before using it.

9) If you do catch a virus, there are antivirus programs to hunt down and … the virus.

10) The problem is that around 150 new viruses appear every month and you must constantly… to deal with these new forms.

VIRUSES AND VACCINES

4. Знаете ли вы, как вести себя в Интернете? Существует ли этика Сетевого Братства?
5. Тащат все: личные коды кредитных карточек, авторские музыкальные произведения, последние компьютерные игры. Хакеры называют это дележкой, остальное — откровенным воровством.
6. Легальный компьютерный бизнес поднимается на свою защиту.
7. Если вы используете компьютер в своем бизнесе, то вы должны иметь антивирусные программы и обновлять их постоянно.
8. Есть два способа избежать заражения компьютерными вирусами: не устанавливать новое программное обеспечение без проверки и не загружать бесплатную информацию из сети.
9. Самыми быстрыми способами нелегального распространения программного обеспечения сейчас являются: воровство, взлом и торговля краденым.

Related Reading

VIRUSES AND VACCINES

The terms *viruses* and *vaccines* have entered the jargon of the computer industry to describe some of the bad things that can happen to computer systems and programs. Unpleasant occurrences like the March 6, 1991, attack of the Michelangelo virus will be with us for years to come. In fact, from now on you need to check your IBM or IBM-compatible personal computer for the presence of Michelangelo before March 6 every year — or risk losing all the data on your hard disk when you turn on your machine that day. And Macintosh users need to do the same for another intruder, the Jerusalem virus, before each Friday the 13th, or risk a similar fate for their data.

A virus, as its name suggests, is contagious. It is a set of illicit instructions that infects other programs and may spread rapidly. The Michelangelo virus went worldwide within a year. Some types of viruses include the *worm*, a program that spreads by replicating itself; the *bomb*, a program intended to sabotage a computer by triggering damage based on certain conditions — usually at a later date; and the *Trojan horse*, a program that covertly places illegal, destructive instructions in the middle of an otherwise legitimate program. A virus may be dealt with by means

of a *vaccine*, or *antivirus*, program, a computer program that stops the spread of and often eradicates the virus.

Transmitting a Virus. Consider this typical example. A programmer secretly inserts a few unauthorized instructions in a personal computer operating system program. The illicit instructions lie dormant until three events occur together: 1. the disk with the infected operating system is in use; 2. a disk in another drive contains another copy of the operating system and some data files; and 3. a command, such as COPY or DIR, from the infected operating system references a data file. Under these circumstances, the virus instructions are now inserted into the other operating system. Thus the virus has spread to another disk, and the process can be repeated again and again. In fact, each newly infected disk becomes a virus carrier.

Damage from Viruses. We have explained how the virus is transmitted; now we come to the interesting part — the consequences. In this example, the virus instructions add 1 to a counter each time the virus is copied to another disk. When the counter reaches 4, the virus erases all data files. But this is not the end of the destruction, of course; three other disks have also been infected. Although viruses can be destructive, some are quite benign; one simply displays a peace message on the screen on a given date. Others may merely be a nuisance, like the Ping-Pong virus that bounces a "Ping-Pong ball" around your screen while you are working. But a few could result in disaster for your disk, as in the case of Michelangelo.

Prevention. A word about prevention is in order. Although there are programs called vaccines that can prevent virus activity, protecting your computer from viruses depends more on common sense than on building a "fortress" around the machine. Although there have been occasions where commercial software was released with a virus, these situations are rare. Viruses tend to show up most often on free software acquired from friends. Even commercial bulletin board systems, once considered the most likely suspects in transferring viruses, have cleaned up their act and now assure their users of virus-free environments. But not all bulletin board systems are run professionally. So you should always test diskettes you share with others by putting their write-protection tabs in place. If an attempt is made to write to such a protected diskette, a warning message appears on the screen. It is not easy to protect hard disks, so many people use antivirus programs. Before any diskette can be used with a computer system, the antivirus program scans the diskette for infection. The drawback is that once you buy this

I. Study the words and word combinations for your better text understanding:

1. **term** – термин;
2. **jargon** [ˊdʒɑ:gən] – жаргон, говор, наречие;
3. **occurrence** – случай, явление, происшествие; распространение; местонахождение;
4. **on you need** – зд. когда вам надо;
5. **a similar fate** – подобная участь;
6. **contagious virus** [kənˊteidʒəs ˊvaiərəs] – заразный, инфекционный вирус;
7. **illicit instructions** [iˊlisit] – запрещенные команды;
8. **to replicate oneself** – зд. копироваться;
9. **to sabotage a computer** [ˊsæbətɑ:ʒ] – зд.выводить из строя компьютер;
10. **to trigger damage** [ˊtrigə] – наносить вред;
11. **legitimate program** [liˊdʒitimət] – законная программа;
12. **to eradicate the virus** [iˊrædikeit] – искоренять, ликвидировать вирус.

Transmitting a Virus

1. **to lie dormant** [ˊdɔ:mənt] – бездействовать;
2. **under these circumstances** [ʌndə ði:z ˊsə:kəmstəns] – при данных обстоятельстельствах;
3. **thus** [ðʌs] – так, таким образом;
4. **a virus carrier** – носитель вируса.

Damage from Viruses

1. **consequences** – последствия;
2. **to erase** – стирать, удалять;
3. **benign virus** – «добрый, мягкий» вирус;
4. **to bounce** – подпрыгивать, отскакивать;
5. **to result in disaster** – (на-) вредить чему-либо.

Prevention

1. **to tend** – иметь тенденцию, быть склонным к чему-либо;
2. **a bulletin board** –доска объявлений;
3. **to assure** – уверять, убеждать; обеспечивать, гарантировать;
4. **to share** – делиться чем-либо;
5. **drawback** – недостаток;
6. **upgrade** – усовершенствование.

II. Answer the following questions:

1. What terms have entered the jargon of the computer industry? **2.** What virus came to be with us for years? **3.** What is it a set of illicit instructions? What can include some types of viruses? **4.** By what means a virus may be dealt with? **5.** About what is it said in typical considered example? Tell about three events. **6.** What is it a virus carrier? **7.** What can do the virus instructions? In what way disk or another drive can be infected? **8.** What can you tell about benign viruses? **9.** What programs are called *vaccines*? **10.** What is it said about bulletin boards? Do all of them run professionally? **11.** What must be done before any diskette can be used? **12.** In what is the drawback?

III. Find the sentences below in the given text:

1. Вирус Микеланджело широко распространился в течение года.
2. Программист скрывает несколько нелегальных команд в операционной системе персонального компьютера.
3. При данных обстоятельствах вирусные команды распространяются на другую оперативную систему.
4. Когда счётчик достигает 4, вирус удаляет все остальные файлы данных.

5. Вирусы имеют обыкновение проявляться чаще всего на свободном программном обеспечении, позаимствованном у друзей.

6. Если предпринимается попытка записи на такую защищённую дискету, на экране появляется предупреждающее сообщение.

IV. Find in the text word combinations with the word “virus” and translate them into Russian.

V. Form nouns – N:

to enter –
to describe –
to happen –
to need –
to check –
to turn –
to suggest –
to infect –
to spread –
to include –
to sabotage –
to stop –
to eradicate –

VI. Form adjectives – Adj:

person –
program –
event –
system –
process –
part –
reach –
file –
end –
result –
prevent –
protect –
act –

VII. Form verbs – V:

occurrence –
attack –
coming –
computer –
calculator –
risk –
user –
intruder –
instruction –
operating –
reference –
counter –
erasure –

VIII. Find the words with negative prefixes.

IX. Translate into Russian in a written way:

1. And Macintosh users need to do the same for another intruder, the Jerusalem virus, before each Friday the 13th, or risk a similar fate for their data.
2. The virus instructions add 1 to a counter each time the virus is copied to another disk.
3. So you should always test diskettes you share with others by putting their write-protection tabs in place.

X. Find the sentences where nouns **V + ing** are used. Write down and translate them.

XI. Write down formulae to the next word combinations. Mind the names of parts of speech:

N – noun (сущ.)	**Adj** – adjective (прил.)	**V** – verb (глагол)	**Adv** – adverb (наречие)

Model: unpredictable conditions – Adj + N

1. computer industry
2. compatible personal computer
3. unpleasant occurrences
4. Jerusalem virus
5. similar fate
6. illicit instructions
7. spread rapidly
8. can happen
9. Macintosh users
10. go worldwide
11. intended to sabotage } program
12. later date
13. damage based on certain} conditions
14. place covertly
15. illegal, destructive } instructions
16. legitimate program
17. lie dormant

XII. Join parts of these sentences:

1. A virus as its name suggests….
2. The *worm* is ….
3. The *Trojan horse* is ….
4. The *bomb* is….
5. A virus may be dealt with by means of….
6. A programmer secretly inserts a few….
7. Thus the virus has spread to another disk…
8. Although viruses can be destructive…
9. The Ping-Pong virus ….
10. It is not easy to protect hard disks, so….

A. a program that spreads by replicating itself.
B. a vaccine, or antivirus, program, that stops the spread of virus.
C. a program that covertly places illegal instructions in the middle of legitimate program.
D. and the process can be repeated again
E. a program intended to sabotage a computer.
F. unauthorized instructions in a PC OS program.
G. is contagious.
H. bounced a ”ball” around your screen.
I. some are quite benign.
J. many people use antivirus programs.

XIII. True / False statements:

1. In fact, from now on you need to check your IBM compatible personal computer for the presence of Trojan horse before March, 6 every year when you turn on your machine.

2. A virus is a set of legal instructions that insert into other programs and help them to work better.
3. The illicit instructions lie dormant until three events occur together.
4. Each newly infected disk becomes a virus carrier.
5. When the counter reaches 4, the virus remains your data and adds its own ones.
6. One of the viruses can simply display a peace message on the screen on a given date.

ENCLOSURE


Все великое
JAVA
DHTML
INTERNET
Интернет – быстро растущее дитя XX века

COMPUTER VIRUS

1. What is it and how to fight it? On this subject, has written dozens of books and hundreds of articles, the fight against computer viruses professionally engaged in hundreds (or thousands) of specialists in dozens (maybe hundreds) of companies. It would seem that this theme is not as complex and challenging to be the object of such attention. However, it is not. Computer viruses have been and remain one of the most common causes of loss of information. There have been cases when the virus blocked the work of organizations and enterprises. Moreover, a few years ago was recorded case where a computer virus caused the death of a man - one of the hospitals in the Netherlands, the patient received a lethal dose of morphine for the reason that the computer was infected by a virus and gave wrong information.

Despite the tremendous efforts of competing anti-virus firms, the losses brought by computer viruses, do not fall down and reach huge quantities in the hundreds of millions of dollars annually. These estimates are clearly too low, since it is known is only a part of such incidents. It should be borne in mind that anti-virus software and "hardware" does not give full guarantee of protection against viruses. Approximately the same bad things on the other side of the tandem of "man-computer". Both users and professional programmers often do not even have the skills of "self-defense and their ideas about the virus often are so superficial that it is better to them (ideas) and was not.

Slightly better things in the West, where more and literature (published as much three monthly magazine devoted to viruses and protect against them), and viruses smaller (because the "Left" Chinese CDs especially do not come on the market), and antivirus companies behave active (conducting, for example, special conferences and seminars for professionals and users). We have, unfortunately, all this is not quite true. And one of the least "worked" items is the literature on the problems of combating viruses. Currently available on store shelves printed virus-wing or obsolete, or written by non-professionals, or authors like Khizhnyak that much worse. Quite unpleasant aspect is also outpacing job of Russian computer "underground": just over two years was issued more than a dozen electronic issues of the journal virus «Infected Voice», has several stations BBS and WWW-pages focused on the spread of viruses and associated information. All this and spurred to bring together all the material that I have accumulated over the eight years of professional work with computer viruses, their analysis and design methods for the detection and treatment.

Compulsory (necessary) property of a computer virus is the ability to create their duplicates (not necessarily coincide with the original) and introduce them to computer networks and / or files, system of a computer and other executable objects. It duplicates retain the ability to further spread.

2. ***History of computer viruses - from antiquity to the present day:***

2.1. *Few archaeological opinions* about the date of birth of the first computer virus very much. I know for one thing: the car Babbage was not there, but on the Univac 1108 and they were IBM-360/370 («Pervading Animal» and «Christmas tree»). Thus, the first virus appeared somewhere in the early 70's or even in the late 60's, though the "virus" no one has ever called. The conversation about the extinct fossil offer be considered completed.

2.2. *Home path*

Let's talk about the latest stories: ***«Brain»***, ***«Vienna»***, ***«Cascade»*** and more. Those who started working for IBM-PC as much in the mid 80's still have not forgotten the rampant epidemic of these viruses in 1987-89 respectively. Letters poured on the screens, and users of the crowd rushed to repair technicians displays (now the opposite is true: Winchester croaked of old age, and knocked on the best science unknown virus). The computer then played the hymn peregrine «Yankee Doodle», but the dynamics of repair, no one rushed - very quickly figured out that it is - a virus, but not one, but a dozen.

This virus started lo infects files. Virus ***«Brain»*** and prancing around on the screen the ball virus ***«Ping-pong»*** a victory over the virus and the Boot-sector. All this is very not like users to IBM-PC, and - there antidote. First got my antivirus was domestic ***ANTI-KOT***: a legendary ***Oleg Kotik*** has published the first version of his program, which destroys the entire four viruses (American SCAN appeared in our country a little-later). By the way, anyone who still retained a copy of the antivirus, I

propose to immediately wipe it (forgive me Oleg Kitty!) Program as harmful, and nothing but wasting of the nerves and unnecessary phone calls, does not bear. Unfortunately, ***ANTI-KOT*** determines virus ***«Time»*** («***Jerusalem"***) by a combination of «MS-DOS» at the end of the file, and some other anti-virus these same letters neatly hooked to all files with the extension of COM or EXE. Attention is drawn to the fact that the conquest of viruses in Russia and the West differ. The first virus has jip read rapidly in the West was a boot virus ***«Brain»***, and only then appeared file viruses ***«Vienna»*** and ***«Cascade»***. In Russia, on the contrary, at first there were file viruses, and a year later - the boot. Time passed, viruses multiplied. They were somewhat similar to each other, climbed into memory, clinging to the files and sectors, periodically kill files, floppy and hard drives. One of the first "revelations" was a virus ***«Frodo.4096»*** - the first that I know of file viruses' invisible (stealth). This virus hooks INT 21h and the treatment through DOS to infected files, edit the information in such a way that the files appear to the user in the uninfected state. But this was only the superstructure of the virus over the VIS-DOS. Less than a year, as electronic cockroaches crawled inside the nucleus DOS (virus-invisible ***«Beast.512»***). The idea of invisibility has continued to bring their fruits and beyond: the summer of 1991 swept, Kosyan computers as bubonic plague, the virus ***«Dir_II»***. ***"Long-aa!»*** Said all those who dug it.

But fight stealth was pretty simple: cleaned the RAM - and be calm, look for reptile and cure his health. Get plenty of trouble brought *self-encrypted viruses*, which sometimes met in regular income in the collection. After all, for their identification and removal had to write special routines to debug them. But this time no one paid any attention until... Not yet emerged a new generation of viruses, those which are known as polymorphic viruses. These viruses use a different approach to invisibility: they are *encrypted* (in most cases), and decryption use the commands that can not be repeated during infection of different files.

2.3. *Polymorphism - the mutation of viruses*

The first polymorphic virus appeared in the early 90's Repository - ***«Chameleon»***, but the real serious problem polymorphic viruses has only a year later - in April of 1991, when virtually the whole world was gripped by a polymorphic virus epidemic ***«Tequila»*** (as far as I know, the epidemic is almost not affected *by Russia*, but Russia first epidemic caused by a polymorphic virus, there was as much three years later - the year 1994, it was a virus ***«Phantom I»***).

The popularity of the idea *self-encrypted* polymorphic viruses has resulted in the emergence of polymorphic code generator - in early 1992 appears the famous virus ***«Dedicated»***, based on the first known polymorphic generator ***MtE*** and opened a series of ***MtE-virus***, and after a fairly short period of time there myself polymorphic generator. He represents himself from the object module (OBJ-file), and now to a very ordinary unencrypted virus get polymorphic mutant need only relink their object modules - OBJ-file polymorphic generator and ***OBJ-file*** virus. Now the author of the virus, if he wishes to create a true polymorphic virus will not have to pore over their own codes for / decryption. If desired, it can connect to your virus polymorphic generator and call it from the code of the virus. Fortunately, the first ***MtE-virus*** does not get to the "wildlife" and did not cause epidemics, and antivirus, respectively, had some lead time to prepare to repel the new scourge. A year later the production of polymorphic viruses have already become *"a craft"*, and in 1993 came their "collapse". In arriving at a collection of viruses share *self-encrypted* polymorphic viruses become more and more. It seems that one of the pillars in the difficult work of creating viruses is the development and debugging of polymorphic mechanism and competition among virus writers are not limited to those who have to write the steepest virus, whose polymorphic mechanism will be all the steeper.

2.4. That is not an exhaustive list of those that can be called absolutely polymorphic (end 1993): ***Boot ache***, ***Civil War (four versions)***, ***Crusher***, ***Dudley***, ***Fly***, ***Freddy***, ***Ginger***, ***Grog, Haifa, Moctezuma (two versions). MVF, Necros. Nuke hard, PcFly (three versions), Predator, Satan bug, Sandra, Shoker, Todor, Tremor, Trigger, Uruguay (eight versions).***

For the detection of these viruses have to use special techniques, which include the emulation to run code of the virus, mathematical algorithms for reconstruction of sections of code and data in the virus, etc. For non-polymorphic hundred percent (i.e., that encrypt itself, but in the decryption of the virus there are always constants bytes) include a dozen new viruses: ***Basilisk, Daemaen***. ***Invisible (two versions), Mirea (multiple versions), Rasek (three versions), Sarov, Scoundrel, Seat, Silly, Simulation***.

However, they require a decryption code for their detection and rehabilitation of affected sites, since the length of the permanent package of decoding these viruses are too small.

In parallel with polymorphic viruses polymorphic generators are developed. Appears a few new ones, using more sophisticated methods of generating polymorphic code, they apply to stations in the BBS in the form of archives that contain object modules, documentation and usage examples. In late 1993, was known for seven generators polymorphic code. This: ***MTE 0.90 (Mutation Engine), four different versions of TPE (Trident Polymorphic Engine), NED (Nuke Encryption Device), DAME (Dark Angel's Multiple Encryptor).***

Since new polymorphic generators appearing for a few pieces a year and bring their full list is hardly worthwhile.

2.5. *Automation and the designers of viruses*

Laziness - the driving force behind progress. This folk wisdom needs no comment. But only in the middle of 1992, progress in the form of automation came to the virus. The fifth of July, 1992 announced for release in light of the first constructor of viral code for IBM-PC compatible computers - Package VCL (Virus Creation Laboratory) version 1.00.

This constructor allows you to generate original and well commented texts viruses (files containing assembly language text), object modules and infected files immediately. VCL is equipped with standard window interface. Using the menu system, you can choose the type of virus being struck by objects (COM and / or EXE), the presence or absence self-encrypts, resistance to the debugger, the internal text strings that connect up to ten effects that accompany the work of a virus, etc. Viruses may use the standard method of destruction of files in their end, or record yourself instead of files, destroying their original contents, or be a virus-satellite (international term - companion viruses [companion]).

And all at once it became much easier: want to play a prank neighbor - and sit for VCL for 10-15 minutes having made 30-40 different viruses, run them on enemy machines. Each computer -separate virus!

2.6. Then, more and more. July, 27th the first version of the constructor PS-MPC (Phalcon / Skims Mass-Produced Code Generator). This constructor does not contain a windows-based interface and generates the source code of viruses on the configuration file. This file contains a description of the virus: type infects tiles (COM or EXE); residency (PS-MPC is also developing and resident viruses, which does not allow the designer VCL); way to install resident copy of the virus, the possibility of using self-encryption; possibility of defeat COMMAND.COM and a lot of other useful information. Based PS-MPC was created by designer G2 (Phalcon / Skim's G2 0.70 beta), which supports the configuration files of the standard PS-MPC, but in the generation of virus uses a greater number of variants encode the same function.

Available in my version of G2 marked the first January, 1993. Apparently, New Year's Eve authors G2 spent at computers. It would be better; instead, they drank champagne, although one does not interfere. So, how it influenced the designers of viruses on e-fauna? In the collection of viruses, this is stored on my «stock», the number of «designer» viruses as follows: based on VCL and G2 - several hundred; based on Intel PS-MPC - more than a thousand.

Let's show another trend in the development of computer viruses: an increasing part of the collections are beginning to "construct" viruses, and the ranks of their authors starting to pour frankly lazy people that bring the creative and respected profession virus-writing to a very ordinary profession.

3. To struggle effectively with viruses, it is necessary to know about "habits" of viruses and to be guided in methods of counteraction to viruses. As a virus is called specially created program capable independently to extend in the computer environment. If the virus has got to the computer together with one of programs or with a document file after a while other programs or files on this computer will be infected. If the computer is connected to a local or global network the virus can extend and further, on other computers. Authors of virus programs create them from different promptings; however results of work of viruses appear, as a rule, similar: infections spoil programs and the documents which are on the computer that often leads to their loss. Some viruses are capable to destroy in general all information on disks of the computers which cost can in tens and hundreds times to exceed cost of the computer.

Uniform classification of viruses does not exist, however it is possible to allocate three basic groups of viruses:

- File viruses;
- Loading viruses;
- The combined file-loading viruses.

LOADING VIRUSES

It is the second big group of viruses they become more active and extend at the moment of operating system loading, still before the user has had time to start any anti-virus program. Computer loading is usually made from a hard disk - the Winchester, and in emergency cases - with system diskettes. The loading order depends on a choice made in program BIOS Setup. The user can specify that the computer should be loaded or only from a hard disk, or from a diskette from the device and if such diskettes are not present, from a hard disk. Other variants depending on concrete realization BIOS (for example, loading from CD-ROM compact disc) are possible also.

Computer loading is made as follows. Right after power supplies inclusions the program of the initialization which have been written down in ROM of base system of input/conclusion BIOS starts to work. It checks operative memory and other devices of the computer, and then transfers control to the program of initial loading which also is in ROM BIOS. Last reads out contents of the very first sector of a zero path of a hard disk in which there is a main loading record Master Boot Record (MBR) in operative memory, or contents of the very first sector of a zero path of the diskette inserted into the disk drive.

This sector contains loading record Boot Record (BR). At loading from a hard disk in memory to the fixed address contents of the main loading record (MBR) - the program of loading of an operating system from a logic disk are read out. The loader looks through the table of sections of disk Partition Table (it is in the same sector of a disk, as record MBR), searches the section noted as active and reads out in operative memory the very first sector of this section, sector of loading record BR. In this sector there is one more loader. Loader VR problem is reading in operative memory of starting modules of an operating system and transfer of management by it. At loading from a diskette this process is much easier, as the diskette format in accuracy corresponds to a format of a logic disk. The very first sector of a zero path of a diskette contains loading record BR, after reading in operative memory to it control is transferred. At what if a diskette - not system, in the first sector of its zero path the program, which unique appointment - a conclusion of the message on necessity to insert into the disk drive system a diskette is all the same written down. And the given circumstance - presence of loading record on not system to a diskette - plays the important role at distribution of loading viruses.

Thus, operating system loading is the multistage process which course depends on different circumstances. Important that is involved in this process three programs which serve as object of an attack of loading viruses:

-The main loading record;
- Loading record on a logic disk,
- Loading record on a diskette.

Viruses can replace some or all listed objects, building in the body and keeping contents of original loading sector in any other, more or place less suitable to it on a disk. At the subsequent inclusion of the computer the loading program brings a virus code in memory and transfers to its control. Operating system loading proceeds under the virus control that complicates and in certain cases and excludes its detection by anti-virus programs.

Loading viruses extend mainly at restart (or inclusion) the computer with forgotten in the disk drive infected with a diskette, then (at loading) the virus gets into the main loading record of a hard

disk of the computer. Therefore it is possible to block completely access to the computer for loading viruses, having disconnected in BIOS Setup possibility of loading from the device a. Besides, it is not necessary to remove without emergency from diskettes protection against record. Especially it concerns distributive diskettes from which installation ON, and to system diskettes is carried out.

COMBINED FILE-LOADING VIRUSES

These most perfect and most dangerous infections use distribution methods, characteristic both for file, and for loading viruses - they write down the body in files and loading records of diskettes and disks. You can receive such virus, or, having loaded the computer with infected diskettes, or, having started the infected file, in any case the result will be equally sad.

BRIEF HISTORY OF COMPUTER VIRUSES

Computers Virus common classification distinguishes three main types of computer viruses. Traditional virus - a program that gets into your computer begins to replicate itself and cause various problems, such as destroying files. Record results achieved virus I Love You, which in 2000 caused damage estimated at $ 8 billion. "Worms" get into computers through a network, forcing the program send e-mail to send letters containing the virus according to the available memory addresses. So, for example, in 2003, acted in "worm" Blaster, which struck more than 1 million computers. "Trojan horse" does not cause direct harm to your computer, but entering into the system, it allows hackers to gain access to the information available to him, databases, allows to intercept computer management, etc. Using the "Trojan horse" QAZ hackers in 2002 had access to classified program codes of Microsoft. Many modern viruses combine all these qualities. For example, such a virus was created So Big, who in August, 2003, has infected about one third of all the letters, distributed by e-mail.

1945. Birth term. Vice Admiral U.S. Navy Grace Murray Hopper (Grace Murray Hopper), directed the Information Department of Naval Staff, faced with the fact that the electron-counting machines (prototypes of modern computers) began to falter. The reason was the moth had flown into one of the relay. Admiral named this problem "beetle" \ bug, using the term used by physicists U.S. and Britain since the late 19th century (he meant any kind of problem in the electrical devices). Admiral also first used the term "getting rid of the beetle" \ debugging, which is now used to describe the actions which aim to troubleshoot your computer.

1949. Hungarian-born American scientist John von Naumann \ John von Naumann developed a mathematical theory of a self-replicating programs. This was the first theory of creation of computer viruses that have caused very little interest among the scientific community.

Approximately 1950. Mathematicians working in the research division of Bell, invented a game: they create the program are selected by each other's computer space. These were the forerunners of viruses.

1963. Head of Computer Laboratory of Advanced Research Projects Agency \Advanced Research Projects Agency (ARPA), John Liklider \ JCR Licklider offered the first elaborate the concept of a computer network.

1969. ARPA created the first computer network ARPANET. To top it connected computers, including non-military laboratories and research centers in the U.S.A.

Late 1960. Appearance of the first virus. In some cases, these were errors in the program, is to ensure that the programs copied themselves, cluttering your hard drive, which reduces their productivity, but it is believed that in most cases, viruses are deliberately created to break down. Perhaps the first victim of this virus, written by a programmer for fun, has become a computer Univax 1108. The virus is called Pervading Animal and infected only one computer - which was created.

1974. A network of Telenet - the commercial version of ARPANET.

1975. Through Telenet distributed first in the history of network virus The Creeper. To counter the virus for the first time in history written by a special anti-virus software the Reeper.

1979. Engineers from the Xerox Research Center created the first computer "worm" \ worm.

1981. Elk Cloner virus affects computers Apple. The virus spread through the "pirate" computer games.

1983. Scientist Fred Cohen \ Fred Cohen of the University of North Carolina introduces the term "computer virus".

1983. The American writer William Gibson \ William Gibson first used the term "cyberspace" \ cyberspace.

1986. For the first time created a virus for the IBM PC - The Brain. Two brothers from Pakistan were its authors.

COMPUTER VIRUSES. THEIR TYPES

WORM VIRUS

A computer worm is a self-replicating computer program. It uses a network to send copies of itself to other nodes (computers on the network) and it may do so without any user intervention. Unlike a virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, if only by consuming bandwidth, whereas viruses almost always corrupt or devour files on a targeted computer.

Worms spread by exploiting vulnerabilities in operating systems. All vendors supply regular security updates [6] (see "Patch Tuesday"), and if these are installed to a machine then the majority of worms are unable to spread to it. If a vendor acknowledges vulnerability, but has yet to release a security update to patch it, a zero day exploit is possible. However, these are relatively rare.

XSS WORMS

XSS Worms exploit a vulnerability known as cross site scripting (or XSS for short) within a website, normally infecting users whereas other users can be infected in a variety of ways depending on the vulnerability.

Cross-site scripting vulnerabilities are commonly exploited in the form of worms on popular social or commercial websites, such as My Space, Yahoo!, Orkut, Justin. TV and Twitter. These worms can be used for

malicious intent, giving an attacker the basis to steal personal information, cookies, and other relevant data regarding the website or the infected visitor.

In the case of the Samy worm, the largest known XSS worm which infected over 1 million My Space profiles in less than 20 hours, the virus author was sued and entered a plea agreement to a felony charge.

WIN 32/ CONFICKER

Win32/Conficker is a worm that infects other computers across a network by exploiting vulnerability in the Windows Server service (SVCHOST.EXE). If the vulnerability is successfully exploited, it could allow remote code execution when file sharing is enabled. Depending on the specific variant, it may also spread via removable drives and by exploiting weak passwords. It disables several important system services and security products and downloads arbitrary files. Worm it has already infected more than 10 million computers worldwide.

On November 21, 2008, the MMPC identified Worm:Win32/Conficker. This worm seeks to propagate itself by exploiting the vulnerability addressed in MS08-067 through network-based attacks. The MMPC added signatures and detection to Microsoft Forefront, Microsoft One Care, and the Windows Live One Care Safety Scanner on the same day.

HISTORY

On November 25, 2008, the MMPC communicated information about Worm: Win32/Conficker.A through their web log.

On December 29, 2008, the MMPC identified the second variant, Worm: Win32/Conficker.B, and added signatures and detection to Microsoft Forefront, Microsoft One Care, and the Windows Live One Care Safety Scanner on the same day. NOTE: Worm: Win32/Conficker.B can be successful against systems that have applied the security update associated with MS08-067.

On December 31, 2008, the MMPC communicated information about Worm: Win32/Conficker.B through their web log.

On January 13, 2009, the MMPC included the ability to remove both Worm: Win32/Conficker. A worm: Win32/Conficker.B in the January 2009 release of the Windows Malicious Software Removal Tool and communicated information about this through their web log. On January 22, 2009, the MMPC provided consolidated technical information about Worm: Win32/Conficker.B on their web log.

On February 12, 2009, the Microsoft Security Response Center (MSRC) released information about domains that Conficker-infected systems try to connect to. Microsoft also announced information on a partnership with technology industry and academic leaders designed to disable domains targeted by Conficker.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Реферативная работа студентов по теме «Вирусы» (Internet).

2. English for Computer Science Students. Учебное пособие.

3. Учебное пособие для студентов-программистов. Сост. Т.В. Смирнова, М.В. Юдельсон. – М.: Флинта; Наука, 2008.

4. И.П. Агабекян. «Английский язык для технических вузов». Учебное пособие. – Ростов/Дон: Феникс, 2001.

5. А.П. Голубев. «Английский язык». Учебное пособие для студентов СПО. – М.: Академия, 2004.

6. А.Л. Луговая. «Современные средства связи». Учебное пособие по английскому языку. – М.: Высшая школа, 2004.

7. Т. Ю. Полякова, Е.В. Синявская, О.И. Тынкова, Э.С. Улановская «Английский язык для инженеров». – М.,: Высшая школа, 2005.