МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ ЕКОЛОГІЧНИЙ УНІВЕРСИТЕТ

МЕТОДИЧНІ ВКАЗІВКИ
до СРС та виконання контрольної роботи №3 з англійської мови

для студентів ІІІ курсу
заочної форми навчання
Напрям підготовки – комп'ютерні науки

Одеса-2014

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ ЕКОЛОГІЧНИЙ УНІВЕРСИТЕТ

МЕТОДИЧНІ ВКАЗІВКИ
до СРС та виконання контрольної роботи №3 з англійської мови

для студентів III курсу
заочної форми навчання
Напрям підготовки – комп'ютерні науки

"Затверджено"
робочою групою методичної
ради "Заочна та післядипломна освіта"

Одеса-2014

МЕТОДИЧНІ ВКАЗІВКИ до СРС та виконання контрольної роботи №3 з англійської мови для студентів ІІІ курсу заочної форми навчання.
Напрям підготовки – комп'ютерні науки

Укладач: Іванченко А.В. - Одеса - ОДЕКУ, 2014 р., с.

МЕТОДИЧНІ ВКАЗІВКИ
до СРС та виконання
контрольної роботи №3
з англійської мови
для студентів III курсу
заочної форми навчання
Напрям підготовки – комп'ютерні науки

Укладач: Іванченко А.В.

Підп. до друку ___.___.2014 Формат 60x84x16 Папір офсетний
Умовн. друк. арк. 3,9 Тираж __ Зам. №
Надруковано з готового оригінал-макету
_____
Одеський державний екологічний університет
65016, Одеса, вул.Львівська, 15

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ ЕКОЛОГІЧНИЙ УНІВЕРСИТЕТ

МЕТОДИЧНІ ВКАЗІВКИ
до СРС та виконання контрольної роботи №3 з англійської мови

для студентів ІІІ курсу

заочної форми навчання

Напрям підготовки – комп'ютерні науки

"Затверджено"
на засіданні робочої групи методичної
ради "Заочна та післядипломна освіта"
Протокол № ___ від__. _____.____р.
Керівник групи
_____ (Степаненко С.М.)
(підпис)

"Затверджено"
Декан заочного факультету
_____ (Волошина О.В.)
(підпис)

"Затверджено"
на засіданні кафедри іноземних мов
Протокол № ___ від__. _____.____р.
Зав.кафедри
_____ (П′янова І.Ю.)
(підпис)

Одеса – 2014

1. ПЕРЕДМОВА

Нормативна дисципліна "Англійська мова" відноситься до гуманітарного циклу освітньо-кваліфікаційного рівня бакалавр і є складовою частиною загальноосвітньої підготовки студентів ОДЕКУ. Практичне володіння англійською мовою є невід'ємним органічним компонентом сучасної підготовки спеціалістів вищими навчальними закладами. Іноземна мова у вищому навчальному закладі являє собою самостійний курс, який має свій зміст та структуру. Загальний обсяг навчального часу для III курсу за фахом «комп'ютерні науки» визначається робочим навчальним планом та становить 8 годин практичної та 86 години самостійної роботи.

Мета вивчення іноземної мови у немовному вузі - підготувати студента до читання літератури за фахом, спілкування англійською мовою в різних видах мовної діяльності, можливості її використання у практичних цілях.

Загальноосвітнє значення вивчення англійської мови визначається тим, що:

1. порівняння двох мовних систем - рідної та іноземної мови - поглиблює філологічні знання студента, змушує більш вдумливо ставитись до явищ рідної мови;
2. вивчення іноземної мови сприяє розвитку пізнавальної та розумової активності студента;
3. отримана іноземною мовою інформація містить різноманітні факти наукового суспільно-політичного та країнознавчого характеру, що допомагає студентові розширювати кругозір.

Загальноосвітня цінність вивчення іноземної мови усвідомлюється студентами за умови правильної організації зв'язків між курсом іноземної мови та спеціальними дисциплінами. У процесі навчання іноземної мови усі види мовної діяльності (читання, мовлення, аудиювання) тісно пов'язані між собою, хоча їх співвідношення на різних етапах навчання різне, що зумовлено метою та умовами навчання, а також відносною складністю видів мовної діяльності, що виконується.

Практична значимість вивчення англійської мови у вищому навчальному закладі полягає в тому, що володіння англійською мовою є:

- ознакою високого професійного та інтелектуального рівня фахівця;
- можливістю проходження виробничої практики за кордоном;
- можливістю навчання та стажування у закордонних вищих навчальних закладах;
- пріоритетним працевлаштуванням;
- необхідністю користування Internet

В результаті вивчення дисципліни "Англійська мова" студенти повинні *знати* особливості фонетичної, граматичної, морфологічної, синтаксичної структури англійської мови, відповідну спеціальну лексику за фахом.

Після вивчення дисципліни ,,Англійська мова" студент має *вміти:*

- читати, перекладати та реферувати оригінальну літературу за фахом для отримання необхідної інформації;
- брати участь в усному спілкуванні іноземною мовою в обсягу матеріалу, передбаченого програмою.

У процесі досягнення практичної мети здійснюються освітні та виховні завдання навчання іноземної мови.

Контроль поточних знань виконується на базі кредитно-модульної системи організації навчання. Підсумковим контролем є екзамен.

2. ЗМІСТ РОЗДІЛУ

Вступ

В умовах значного розширення міжнародних зв'язків України знання іноземних мов спеціалістами різних галузей науки набувають особливого значення. Одне з головних завдань яке ставиться перед студентами вищих закладів освіти України є практично - комунікативне володіння іноземною мовою на професійному та побутовому рівнях. В процесі практичного володіння іноземною мовою основний наголос робиться на усне мовлення як основну виховну форму мовленнєвої діяльності. ***Письмове мовлення*** — читанням і письмом студенти оволодівають вже на базі засвоєного усного мовлення. Усне мовлення є не тільки метою навчання, але є засобом досягнення цієї мети.

Навчання усім видам мовленнєвої діяльності ведеться комплексно. Усі відомості теоретичного характеру з ***фонетики**** техніки читання та перекладу, граматики даються в процесі практичної роботи в об'ємі потрібному для набування студентами відповідних умінь і навичок.

Значна увага в навчальному процесі впродовж всього курсу приділяється в постановці вимови, особливо інтонації.

Граматична система іноземної мови засвоюється студентами за допомогою граматичних структур усного і письмового МОВЛЕННЯ. Порядок подання граматичних структур визначається послідовністю поступового ускладнення матеріалу і залежності його від попереднього матеріалу.

Лексика - слова, словосполучення і вирази засвоюються в мовленні в їх природному матеріалі.

Вільне спілкування іноземною мовою можливо лише коли студенти будуть мислити цією мовою. Тому розвиток мислення іноземною мовою є

важливим завданням практичного курсу, що забезпечується численними, різноманітними мовними оригінальними вправами і створення мовної атмосфери на заняттях поза аудиторний час.

Знання:

- вимови усіх звуків англійської мови на рівні комунікативної достатності (рівень розбірливості для усного спілкування) та основними інтонаційними моделями;
- закономірностей англійської мови у співставленні її з діловою українською мовою;
- фонетичного, граматичного, лексичного, морфологічного, синтаксичного мінімуму передбаченого програмою кафедри іноземних мов ОДЕКУ з англійської мови.

Вміння:

- вести бесіду на основі типових ситуацій ділового спілкування, у зв'язку з прочитаним або прослуханим;
- робити повідомлення на основі типових ситуацій ділового спілкування, а також висловлюватися з приводу прочитаного або прослуханого;
- самостійно читати (зі словником) суспільно-політичні, науково-популярні тексти, а також за фахову літературу;
- сприймати на слух при безпосередньому спілкуванні та у
- звукозапису тексти побудовані в основному на засвоєному мовному матеріалі.

Структура дисципліни „Англійська мова". Розподіл граматичного і лексичного матеріалу в межах семестру, кількості годин, які необхідні для засвоєння певних граматичних і лексичних тем студентами заочного відділення III курсу, визначається кафедрою іноземних мов у робочих навчальних планах на основі програми з іноземних мов. Вивчення курсу розраховане на 92 години, із них 6 годин аудиторних занять, 86 годин на самостійну роботу студентів.

Для виконання контрольних робіт треба вивчити такі теми III курсу заочної форми навчання:

1. Особливості перекладу видо-часоних форм дієслів (Active Voice).
2. Особливості перекладу видо-часових форм дієслів (Passive Voice).
3. Особливості перекладу модальних дієслів
4. Особливості перекладу інфінитива.
5. Особливості перекладу дієприкметників.
6. Особливості перекладу герундія

7. Особливості перекладу дієслів з після-логами. Особливості перекладу суспільно-політичного тексту.
8. Особливості перекладу іменників з прийменниками. Особливості перекладу суспільно-політичного тексту.
9. Особливості перекладу прикметників з прийменниками. Практика у перекладі.
10. Практика у перекладі суспільно-політичного тексту та тексту за фахом.

ДИСТАНЦІЙНА ФОРМА НАВЧАННЯ

Згідно з вимогами покращення навчального процесу та впровадження нових видів та форм навчання, які, серед іншого, мають на меті використання його дистанційної форми, студенти мають можливість виконувати та надсилати контрольну роботу частинами згідно з нижче наведеним графіком.

Графік виконання контрольної роботи

I завдання – вересень-жовтень;
II завдання – листопад;
III завдання – грудень;
IV завдання – січень;
V завдання – лютий;
VI завдання – березень;
VII, VIII завдання – квітень.

ОРГАНІЗАЦІЯ ПОТОЧНОГО ТА ПІДСУМКОВОГО КОНТРОЛЮ ЗНАНЬ

Поточний контроль здійснюється на протязі навчального курсу (семестру) за наступними формами:

- перевірка контрольної роботи, яка виконується у міжсесійний період;
- перевірка знань та вмінь студента під час аудиторних занять протягом заліково-екзаменаційної сесії.

Максимальна сума балів, яку може отримати студент за кожний захід поточного контролю не регламентується, а визначається викладачем. Сума міжсесійної та сесійної оцінки (ОМ + ОЗЕ) складає загальну оцінку поточного контролю.

Студент вважається допущеним до підсумкового семестрового контролю з конкретної навчальної дисципліни, якщо він виконав всі види робіт поточного контролю, передбачені робочою навчальною програмою дисципліни і набрав за накопичувальною системою суму балів не менше

50% від максимально можливої за дисципліну, своєчасно виконав міжсесійні контрольні роботи.

Підсумковим контролем є іспит, а допуском до іспиту є наявність контрольної роботи № 3.

В дисципліні "Англійська мова", що читається для студентів III курсу заочної форми (напрям підготовки – комп'ютерні науки) навчання у VI семестрі використовується 1 контрольна робота та переклад суспільно-політичного тексту у обсязі 10 000 друк. знаків з практичної частини, в якості форми поточного контролю – усне опитування. Це відповідає 1 заліковой одиниці:

1 залікова одиниця – 6 семестр.

Поточна та підсумкова оцінка знань студентів здійснюється за модульно-накопичувальною системою. Максимальна сума балів, яку може набрати студент, складає 100 балів, з них за контрольну роботу – 20 балів, переклад суспільно-політичного тексту (газета) в обсязі 10 тисяч друкованих знаків – 20 балів, з практичної частини – 60 балів. Мінімальна сума балів, яку може набрати студент, складає 60 балів, з них за контрольну роботу – 20 балів, переклад суспільно-політичного тексту (газета) в обсязі 10 тисяч друкованих знаків – 20 балів, з практичної частини – 20 балів.

Практична частина курсу складається з 2 змістовних модулів, що відповідає розділам робочої програми дисципліни та складається з теоретичної та практичної частин. Теоретична частина оцінюється за наявністю письмових контрольних робіт, а практична – за результатами усного опитування на практичних заняттях.

Модульно-накопичувальна система оцінки знань студента включає:

- систему оцінювання самостійної роботи студента (СРС) у міжсесійний період (ОМ) (контрольна робота);
- систему оцінювання СРС при проведенні практичних модулів дисципліни під час заліково-екзаменоційної сесії (ОЗЕ);
- систему накопичувальної підсумкової оцінки засвоєння студентом навчальної дисципліни (ПО).

Накопичена підсумкова оцінка засвоєння студентом заочної форми навчання навчальної дисципліни розраховується так:

$$\boldsymbol{ПО} = 0{,}5\boldsymbol{ОПК} + 0{,}25\boldsymbol{ОЗЕ} + 0{,}25\boldsymbol{ОМ}$$

де:

ОПК – кількісна оцінка (у відсотках від максимально можливої) заходу підсумкового контролю (***іспит***).

ОЗЕ – кількісна оцінка (у відсотках від максимально можливої) заходів контролю СРС під час проведення практичних модулів.

ОМ – кількісна оцінка (у відсотках від максимально можливої) заходів контролю СРС у міжсесійний період.

При оцінці заходів контролю СРС під час проведення практичних модулів (ОЗЕ) за період сесії ураховується:

- Ритмічність роботи студента на протязі занять (присутність його на заняттях за розкладом).
- Повнота та якість розкриття окремих тем.
- Оцінка захисту окремих розділів та завдань у цілому.

Оцінка виконання СРС у міжсесійний період (ОМ), визначається шляхом перевірки контрольних робіт, передбачених програмою дисципліни, при визначенні якої враховується наступне:

- Відповідальність кількості контрольних робіт навчальній програмі.
- Термін представлення контрольної роботи (на протязі семестру, перед початком заліково-екзаменаційної сесії, безпосередньо перед датою контролюючого заходу).
- Оформлення контрольної роботи згідно ДОСТУ.
- Відповідність змісту роботи її темі.
- Оцінка захисту контрольної роботи.

Підсумковий семестровий контроль (ОПК) передбачає дві форми оцінювання успішності засвоєння студентом навчального матеріалу дисципліни:

- кількісна оцінка (бал успішності);
- якісна оцінка.

Кількісна оцінка (бал успішності) – це відсоток, який становить інтегральна сума балів, отриманих студентом на контролюючих заходах, по відношенню до максимально можливої суми балів, що встановлена робочою програмою дисципліни.

Якісна оцінка – це оцінка, яка виставляється на підставі кількісної оцінки (бал успішності) за будь-якою якісною шкалою. На цей час в університеті використовується чотирьохбальна шкала якісних оцінок:

- ***чотирьохбальна*** (відмінно, добре, задовільно, незадовільно) – для форми семестрового контролю у вигляді семестрового іспиту;

Перехід від кількісної оцінки до якісної оцінки здійснюється згідно «Положення про організацію самостійної роботи, поточний та підсумковий

контроль знань студентів в Одеському державному екологічному університеті»:

Сума балів	Якісна оцінка з іспиту	
< 60	незадовільно	
60-73,9	задовільно	
74-89,9	добре	
90-100	відмінно	

ОРГАНІЗАЦІЯ ПРАКТИЧНИХ ЗАНЯТЬ

Після практичних модулів студенти повинні оволодіти наступними базовими *вміннями та знаннями:*

- охарактеризувати умовний спосіб в англійській мові;
- пояснити структуру та особливості вживання трьох типів речень в умовному способі;
- пояснити вживання інфінітива та його форм в англійській мові;
- пояснити вживання дієприкметникових зворотів в англійській мові;
- читати, перекладати та переказувати тексти суспільно-політичної тематики;

читати, перекладати та переказувати тексти за фахом.

КОНТРОЛЬНА РОБОТА № 3
ВАРІАНТ №1

I. Translate this text in writing:

Text **TYPES OF COMPUTER SECURITY**

Computer security is that branch of information technology which deals with the protection of data on a network or a stand-alone desktop. As every organization is dependent on computers, the technology of its security requires constant development. Here are the different types of computer security.

Hardware Security

Threat

Even if the computer is not plugged into a network, a person can open its cabinet and gain access to the hard drives, steal them and misuse or destroy the data saved on them or, damage the device altogether. It is also necessary to remember that in case one dissembles his computer hardware, the risk of losing coverage of warranty becomes very high.

Protection

The security of computer hardware and its components is also necessary for the overall protection of data. If a stand-alone system contains some important or classified information, it should be kept under constant surveillance. Locking system for a desktop and a security chain for a laptop are basic security devices for your machine. Certain disk locks are available in various sizes, which control the removal of the CPU cover protecting internal components of the system. For example, you will find disk/tape drive lock, computer case lock with cable and padlock, security cables, etc. A disk lock guards all the internal access points located on the CPU and protects them.

Software Security

Network Security

Computer networks are an integral part of any organization these days, as they facilitate the free flow of data and services to the authorized users. However, such networks also pose a security threat in case the data is classified and confidential, thus making network security a vital necessity.

Threats

As the data is available only for authorized users, it is possible for hackers to pretend to be one, by providing the correct user name and password. Computer network security can be disrupted or encroached in the following ways:

Denial of Service

Denial-of-service is meant to disable a computer or a network and can be executed with limited resources. It is one of the most common forms of attacks by hackers and can effectively disable the whole network of an organization. Denial of service attack makes a computer resource unavailable to its intended user. To carry out this kind of attack, hackers generally flood a network or the

access routers with bogus traffic. They also make attempts to disrupt connections between two machines and prevent individuals from accessing a service.

Trojan Horse

Trojan horse is common and one of the most potential threats to computer security. They are malicious and security-breaking programs, disguised as something which is considered as non-malicious by the security software. They are a useful tool for hackers who try to break into private networks. Hackers generally attach Trojan horse to a file, which triggers a virus or remotely controlled software, giving the hacker complete control over the computer.

Viruses and Worms

Viruses and worms are well-known for their destructive nature and the property of replicating themselves. They are basically pieces of computer program codes, which are written by hackers and other computer geniuses.

Sniffing

Sniffing is the act of intercepting TCP/IP packets while they are getting transferred on a network. The interception generally takes place through simple eavesdropping done by a hacker.

Protection

Firewall

It is one of the most essential type of network security in today's world of Internet. Firewall is a filter that prevents fraud websites from accessing your computer and damaging the data. However, a firewall is not a great option for securing the servers on the Internet because the main objective of a server is granting access to unknown users to connect to various web pages.

Security Software

Along with firewall, try installing a good anti-virus and security software to enhance the security level of your computer system.

Data Security

Threat

Although uncommon, hardware malfunction can prove to be a major threat to your data in the computer. The life span of hard disks is always limited because of surrounding factors and this can amount to a severe loss of all your files saved on the disk, if there is no proper backup of those files made on any other system.

Protection

Keep Backup

It is important to avoid data and information loss in case of hard disk crashes. The only solution is to regularly keep backups of all the data on other media such as magnetic tapes, CD-ROM, etc. It is a good practice to store the media off-site and in case of a disk crash, restore the information from the backup media onto the new disk. In case a backup media is not affordable, one should

try to store the files on at least two different media devices. These media devices should be systematically kept at a place which is safe and secured, as the information contained may be confidential. People usually have backup for database files, spreadsheet files and large documents. As the technical constraints are always there, it is better to take regular backups, in order to avoid any loss of information.

Clean-up Software

Install a software program on your computer that will clear all the old, unused files and registry keys. It will also help to detect malware and save your computer from a severe damage caused by it. Keep your system in the loop of latest updates and security alerts or else, it will become vulnerable to security threats.

It is important to keep a record of technical support consultants and software documentations, like manuals and guides to make them accessible to the staff members of the company.

II. Put 5 questions to the text.

Example: What main types of computer security do you know?

КОНТРОЛЬНА РОБОТА № 3

ВАРІАНТ №2

I. Translate this text in writing:

Text **HOW DOES A COMPUTER KEYBOARD WORK?**

A computer keyboard is a hardware device that functions in accordance to the instructions provided by the user. It comprises circuits, switches, and processors that help in transferring keystroke messages to the computer.

Did You Know?

The current keyboard layout, or the QWERTY layout, which is based on the layout of the typewriter keyboard, was designed not to increase the speed of typing, but to slow it down, to avoid typewriters from jamming.

In today's technology-driven world, everyone is aware about computing, and how to use a computer. We all know that the keyboard is an input device that functions in accordance to the instructions of the user. Computer keyboards are used for preforming various tasks, such as typing on a word processor or text editor, accessing menus, and playing games. In this article, we take a closer look at how computer keyboards work.

The Computer Keyboard Explained

The computer keyboard was modeled in the 1940s based on the technology of a typewriter keyboard. In general, most computer keyboards contain 80 to 110 keys, depending on the OS, the manufacturer, or the application it is made for.

These include function keys, typing keys, numerical keys, and control keys. Here is a picture of the most common type of computer keyboard.
In the picture, the top row (F1-F12) are the function keys, the second row are the numerical or number keys, the 3rd, 4th, and 5th, rows are the typing keys, while the last row contains the command keys.
In addition to these, a keyboard also contains other modifier keys, like Shift, and a numerical pad on the right to make inputting numbers easier.
How Computer Keyboards Work
When you type, or press any keys on the keyboard, a processor analyzes the position of the keys pressed, and sends this information to the computer, where it is sent to something called the 'keyboard controller'. The keyboard controller processes the information that is sent by the keyboard's processor, and, in turn, sends it to the operating system. The OS then checks this data to analyze if it contains any system level commands, like Ctrl+Shift+Esc, which is the keypress to bring up the Task Manager. If such system level commands are present, the computer executes them, if not, it forwards the information to the current application. The application then checks if the keypresses relate to commands in the application, like Ctrl+P, which is the keypress for the print command. Again, if there are such commands, they are executed first, and if not, then these keypresses are accepted as content or data. All of this happens in a fraction of a second, so even if you press many keys, there is no lag in the system.
So, how are these keypresses detected? Well, to put it simply, keyboards use switches and circuits to change keystrokes to a format the computer understands. Every keyboard contains a processor that does the work of translating the keystrokes, or the keys pressed, to the computer.
If you open a computer keyboard, you will see a small processing unit, and large circuit board. It is this circuit board, along with the processor, that enables the computer to understand what you are typing. This board, also known as the key matrix, is placed under the keys, and is broken at a specific point under every key, which results in making the circuit incomplete. When you press any particular key, it completes this circuit, thus enabling the processor to determine the location of the key that was pressed.

The key matrix under the keys has a corresponding chart or character map that is stored in the read-only memory (ROM) of the computer. When you press a key, the processor looks up the position of the circuit that was closed, or completed, with the character map, and determines which key was pressed. All the keys are mapped and stored in the memory. For example, in the character map, if just the location of the 'x' key is determined to be pressed, then the resulting lower case alphabet 'x' will be displayed or taken as a keypress, but if the locations of the 'Shift' and 'x' keys have been determined to be pressed, then the resulting uppercase character 'X' will be displayed or taken as a keypress.

Mechanical and capacitive are the two types of switches that are used to complete circuits in keyboards. Some keyboards, instead of using the mechanical process described above, use a capacitive process. In this process, the circuit is not broken and current passes through it continuously. However, each individual key has a plate attached to it that moves closer to the circuit when pressed. This movement registers with the key matrix, causing a change in the electric current flowing through the circuit. This change is then compared to the character map, and the location of the key pressed is determined.

Mechanical switches include rubber dome switches, membrane switches, metal contact switches, and foam element switches. Of these, rubber dome switches are the most common, as they have a good tactile response and are fairly resistant to spills and corrosion, in addition to being relatively inexpensive and easy to manufacture.

Though there are various types of keyboards, like wireless, Bluetooth, and USB keyboards, they all use the same principle, of completing a circuit to determine a keypress, to work.

II. Put 5 questions to the text.

Example: What is computer keyboard?

КОНТРОЛЬНА РОБОТА № 3

ВАРІАНТ №3

I. Translate this text in writing:

Text ADVANTAGES AND DISADVANTAGES OF COMPUTER NETWORKS

A computer network is a set of electronically connected computers which can share information and resources among themselves. There are communication protocols that define how this sharing should take place.

Like every other technological prospect, computer networks come with its set of advantages and disadvantages.

Advantages of Networks

File Sharing

The major advantage of a computer network is that is allows file sharing and remote file access. A person sitting at one workstation that is connected to a network can easily see files present on another workstation, provided he is authorized to do so. This saves him/her the hassle of carrying a storage device every time data needs to be transported from one system to another. Further, a central database means that anyone on that network can access a file and/or update it. If files are stored on a server and all of its clients share that storage capacity, then it becomes easier to make a file available to multiple users.

Resource Sharing

Resource sharing is another important benefit of a computer network. For example, if there are twelve employees in an organization, each having their

own computer, they will require twelve modems and twelve printers if they want to use the resources at the same time. A computer network, on the other hand, provides a cheaper alternative by the provision of resource sharing. All the computers can be interconnected using a network, and just one modem and printer can efficiently provide the services to all twelve users.

Inexpensive Set-Up

Shared resources mean reduction in hardware costs. Shared files mean reduction in memory requirement, which indirectly means reduction in file storage expenses. A particular software can be installed only once on the server and made available across all connected computers at once. This saves the expense of buying and installing the same software as many times for as many users.

Flexible Handling

A user can log on to a computer anywhere on the network and access his files. This offers flexibility to the user as to where he should be during the course of his routine. A network also allows the network administrator to choose which user on the network has what specific permissions to handle a file. For example, the network administrator can allot different permissions to User A and User B for File XYZ. According to these permissions, User A can read and modify File XYZ, but User B cannot modify the file. The permission set for User B is read-only. This offers immense flexibility against unwarranted access to important data.

Increased Storage Capacity

Since there is more than one computer on a network which can easily share files, the issue of storage capacity gets resolved to a great extent. A standalone computer might fall short of storage memory, but when many computers are on a network, the memory of different computers can be used in such a case. One can also design a storage server on the network in order to have a huge storage capacity.

Disadvantages of Networks

Security Concerns

One of the major drawbacks of computer networks is the security issues that are involved. If a computer is a standalone computer, physical access becomes necessary for any kind of data theft. However, if a computer is on a network, a hacker can get unauthorized access by using different tools. In case of big organizations, various network security software need to be used to prevent theft of any confidential and classified data.

Virus and Malware

If even one computer on a network gets affected by a virus, there is a possible threat for the other systems getting affected too. Viruses can spread on a network easily, because of the inter-connectivity of workstations. Moreover, multiple systems with common resources are the perfect breeding ground for

viruses that multiply. Similarly, if malware gets accidentally installed on the central server, all clients in the network that are connected to that server will get affected automatically.

Lack of Robustness

If the main file server of a computer network breaks down, the entire system becomes useless. If there is a central linking server or a bridging device in the network, and it fails, the entire network will come to a standstill. In case of big networks, the file server should be a powerful computer, which often makes setting up and maintaining the system doubly expensive.

Needs An Efficient Handler

The technical skills and know-how required to operate and administer a computer network is considerably high. Any user with just the basic skills cannot do this job. Also, the responsibility that comes with such a job is high, since allotting username-passwords and permissions to users in the network are also the network administrator's duties. Similarly, network connection and configuration is also a tedious task, and cannot be done by an average user who does not have advanced knowledge of computers and/or networking.

Lack of Independence

Since most networks have a centralized server and dependent clients, the client users lack any freedom whatsoever. Centralized decision making can sometimes hinder how a client user wants to use his own computer.

Computer networks have had a profound effect on the way we communicate with each other today, and have made our life easier. From the World Wide Web to your local office LAN, computers have become indispensable in daily life, and networks have become a norm in most businesses. If networks are designed and configured keeping in mind its pros and cons, they are the best piece of facility you could ever have.

II. Put 5 questions to the text.

Example: What are the advantages of networks?

КОНТРОЛЬНА РОБОТА №3

ВАРІАНТ №4

I. Translate this text in writing:

Text **HOW DOES FACEBOOK WORK?**

Unlike other social networking websites, it may be difficult to find people with the same kind of interests as you have. But Facebook is indeed, one of the best networks to get in touch with long-lost friends. The original intention of Facebook was to connect college students with each other, and let them stay in touch. However, the website became so popular that today, anyone from any part of the world can join it. You can use this website to chat with your friends, date people, share pictures, spread any topic of interest, and meet new people. Now that you have got a brief idea, let's take a look at how to get started.

Starting Up on Facebook

Facebook started out a virtual space created by Harvard freshman Mark Zuckerberg as just something to help his friends communicate with each other. On Facebook, you are able to create a homepage of your own and network with millions of users all around the world. Once you become a member, you are permitted to send an invitation to friends and relatives to join your network. Once they have accepted your invitation, you can suggest the names of people in your network to your newly added friends. Whenever you visit your homepage, you can change and update your current status, and share whatever you are doing with your friends. The best part is that your friends would be able to see whatever you feel, and write to you the next time they log in. Moreover, they can write a comment and send a private message on what they feel about your update. Besides this, you can share website links and videos, and take a look at the links, videos, and photos which your friend have posted. These can be seen only by your selected group of friends. What's more, you could create a group where people who share the same interests can join in, and have discussions.

Signing Up for Facebook

More than 60% of the total Facebook users are older than 35 years.The first step to be a part of this mammoth social networking website is to sign up. You just need to sign in your details like your name, birthday, gender, and your email address. The email address is not published, and for security reasons, can only be used to forward any messages which other people may have sent you. Once you have filled all the information, click on the sign-up icon. A security code appears (captcha code used to prevent spamming software) which you have to enter in order to confirm your signing up. You will then get a confirmation of your account in the email address you have provided.

How to Start Connecting With People

Facebook currently has more than a billion users, half of which log in at least once a day.When you get the confirmation link that is sent to your email address, you need to click on it, and once you do that, you'll be directed to the 'Getting Started' page. Facebook will immediately use the info that you gave it, ranging from your school and/or college, your location, and if you've been invited to join by someone you know, relevant contacts from their friends list.

Facebook has been programmed to ask whether you want it to search your email's contact list. If you opt to go ahead and allow Facebook to search for people, it would search for those people who are your email contacts, and will check if they are on Facebook. If there is anyone on Facebook who is also there in your email list, the website would suggest you those names. You can opt to add them in the list of your friends, and have the freedom to not include anyone you don't wish to.

Start Networking

If you know friends from your school or your colleagues who are already on Facebook, you can add them by first searching for them and then sending an invitation. They need to accept your invite and once accepted you can start networking with them by sending messages, pictures, videos, etc. Moreover, it gives you the option to add or ignore a person from being your friend. Once these steps are done, it means you have successfully created a Facebook profile, and are ready to keep in touch with your friends.

Keep Updating

Once you have created a profile, you can choose to keep it updated so that people know what you have been up to. You can add photos (one profile picture and then multiple albums/photos of anything that you want to show) and share information which you want. You can also set preferences to as much or as little information you want to share with people who are not in your list of friends.

The Intrinsic Workings of Facebook

Now that we know how Facebook works for us, here's what actually happens. A little behind the scenes look at the back-end to front-end working of the biggest social networking site on Earth.

To be concise, Facebook uses the all-powerful LAMP stack, a simple, open source, and fast scaling stack that allows Facebook to do what it does. LAMP basically stands for:

Linux
Apache
MySQL
PHP

What this means is that Facebook uses a stack, that acts as the entire front-end, which communicates with the back-end (Facebook Headquarters) and the user to give you what you want. You can draw parallels to any normal server like so:

Linux is the computer system kernel that forms the operating system. Linux is preferred because it is faster, free (open source), and highly secure (almost impervious to hacking attempts).

Apache is the FTTP server that Facebook uses Linux on.

MySQL is the database language. Facebook uses MySQL to segregate data according to where on Earth it's coming from. This helps in keeping location based information smooth and efficient.

PHP becomes the web programming language, on which the front-end of the site is built. Whatever parts of Facebook you see on your computer, are all made using PHP.

Finally, Memcached becomes the RAM for Facebook. With truckloads of data transactions happening between users every second, they need something that will temporarily store data. Using Memcached makes the workload much lighter on Facebook's front-end. All in all, everything that Facebook uses is free and open sourced. Wikipedia is another website that uses the LAMP stack.

The back-end of Facebook uses a very simple need-based frame development procedure to create something only when it's needed. For instance, if you were to create a new group, it would be created instantly because of the fast need-based programming. For its back-end, Facebook uses Thrift as its protocol, Cassandra as the database management system, and Scribe as its data log server.
So, with Facebook, you can connect with your friends, family, and acquaintances. You have the freedom to choose or ignore any person you want. Once you know how to do this, you can enjoy and have a lot of fun out there. You can also play a few games, such as Farmville, Mafia Wars, Crazy Taxi, and many more. So go ahead and try it, chances are you'll enjoy it soon enough.

II. Put 5 questions to the text.
Example: Who did start out Facebook?

КОНТРОЛЬНА РОБОТА №3
ВАРІАНТ №5

I. Translate this text in writing:

Text **WHO INVENTED THE COMPUTER?**

Ever wondered who invented the machine that allows you to read these very words while listening to music, maintaining a social profile and shooting at a bunch of terrorists, all at the touch of a button? Read on to know more about the inventor of the computer.
The history of computers, in the literal sense as 'computing machines', can be stretched back to abacuses, slide rules, and other similar calculators of the ancient world. The first programmable computer was created by Charles Babbage (December 26, 1791 - October 18 1871) in 1833.
Due to his invaluable invention, Babbage (shown in the adjoining image) is considered the Father of the computer.
This early computer was nothing like the ubiquitous digital giants of today. In fact, since neither electricity nor computer scripting languages had been invented, Babbage's design was mechanical; it had to be operated by various cranks and levers rather than simply pushing a button.
The image (below) shows Babbage's creation (click on the image for better viewing).
Charles Babbage's father, Benjamin Babbage, was a rich businessman. Thus, young Charles went to many prestigious schools and was home-tutored before he went to Holmwood Academy in Enfield. This is where his romance with mathematics began.
Later, he went to Peterhouse, Cambridge for further studies. At Peterhouse he studied analytical philosophy and continued studying mathematics. He never graduated with honors, and was conferred an honorary degree in mathematics without examination.

Apart from being a gifted mathematician, Babbage was also a philosopher and an avid amateur cryptographer. He was also reported to be heavily influenced by the Indian system of logic.
Babbage noticed that the calculations made by the human 'computers', especially regarding logarithms, were often incorrect. This gave him the idea of a machine capable of doing the calculations, intrinsically without the human margin of error. Ada Lovelace, who helped Babbage program his machine, is considered as the first computer programmer in the world.
Interestingly, the history of programming itself doesn't begin with Babbage's 'Analytical Engine'. The first programmable device in the world was actually a loom! Invented by Joseph Marie Jacquard, the Jacquard Loom was the first ever programmable machine.
The programming in both, the Jacquard loom and Babbage's computer, was done through punched cards. Babbage also invented a mechanical forerunner of the printer as the output device for his machine.
The adjoining illustration shows a man punching cards to be used to program the loom (click on the image for better viewing).
The next leap forward in the history of computers came in the form of Konrad Zuse and John Atanasoff's contemporaneous but varied designs. Atanasoff built the first digital computer in the world using vacuum tubes -- the Atanasoff-Berry Computer, laying the groundwork for what would become one of the most useful and common devices in the world. However, Atanasoff's computer was not programmable. On the other hand, Konrad Zuse had built a programmable computer, known as the Z3, which was electromechanical, i.e, analog.
Despite the respective shortcomings of their designs, Atanasoff and Zuse are both considered among the most important names in computer technology and, due to the disparity between their designs, among the inventors of the computer itself. George Stibitz is also considered among the inventors of the digital computer.
The numerous input, output and peripheral devices attached to modern computers were not part of these early designs. They were invented by the following scientists:
Monitor (Cathode Ray Tube): Allen DuMont (1931)
Mouse: Douglas Engelbart (1963)
QWERTY Keyboard: Christopher Sholes (1867 - on typewriters)
Scanner: Giovanni Caselli / Edouard Belin (1858 / 1913)
Charles Babbage couldn't help tinkering with his designs, always striving for the betterment of his devices. But constrained by the technology of the time, the analytical engine never got to the level of sophistication Babbage desired. In 1991, a fully functioning model of his difference engine was constructed, showing the prognostic inventor's true brilliance. The model also promoted research into the possible applications of mechanical computing, which can be

very helpful in situations where digital computers cannot tolerate the physical conditions. In 2011 British scientists initiated a project to build the analytical engine to the best of Babbage's original designs, intended to be completed by 2021. That would indeed be a fitting tribute to the man who set the world on the ongoing journey of unimaginable technological advancement.

With the escalating popularity and usability of the Internet, it is only normal that issues like Internet security or Internet safety are being discussed. Other than hackers and spammers, even pedophiles (online predators) and cyber-terrorists are lurking on the Internet in search of easy prey. If you are wondering why everybody is increasingly talking about Internet security and the need to ensure Internet safety while surfing the virtual world, some information on the threats that you are likely to face in the cyberspace will help you get rid of your doubts.

II. Put 5 questions to the text.

Example: Who did invent the first programmable computer?

КОНТРОЛЬНА РОБОТА №3

ВАРІАНТ №6

I. Translate this text in writing:

Text **WHY IS INTERNET SAFETY SO IMPORTANT?**

There's nothing new about hackers breaking into systems, or fraudulent acts, like identity theft and piracy, in the cyberspace. If at all there is something to be worried about, it is the rate at which these things are happening of late and that's why it's necessary to know why Internet safety is important.

In order to understand why you need to safeguard your privacy and maintain Internet safety standards, it is very important to be aware of the dangers or risks associated with unsecured Internet access. So let's discuss some of the most common issues in Internet safety:

Unauthorized Network Access or Hacking

Unauthorized access is one of the major threats as far as Internet safety is concerned. Network security consists of the provisions made in an underlying computer network infrastructure to protect the network and the network-accessible resources from unauthorized access. Hacking means people can get unauthorized access to your account, computer, or network. Once they have the access to your account, they have complete control over all your transactions, and can misuse your account for illegal or objectionable purposes. A hacker getting access to your online banking account is as good as a robber getting access to your safe.

In March 2012, FBI Director, Robert Mueller revealed that hacking would overshadow terrorism as the biggest threat for the nation in the near future. While 50 per cent of the hacking cases in the US are attributed to hacktivism, a whopping 40 per cent are attributed to cybercrimes.

Phishing, Email Frauds, and Spamming

Phishing refers to the cases of online scams wherein people fraudulently acquire sensitive information by posing as a trustworthy entity via email or instant messaging. Often this information can include your important financial as well as personal contact details. The information can then be used for several illegal purposes, which, in turn, can put you in trouble. At times, this information is collected and sold to online advertisers as well. Online scams, which involve requests for your bank account numbers, passwords, or any other sensitive information, are a menace over the Internet. Spamming might be relatively harmless, but it is just as annoying since it floods your mailbox with unwanted advertising. Spammers are also likely to sell your address and phone numbers, as a result of which you might end up getting bombarded with telemarketing calls and snail mail at times.

RSA Security LLC, formerly known as RSA, is a reputed computer and network security company based in the United States. If the data revealed by them in July 2012 is to be believed, the worldwide monetary losses from phishing alone accounted for over US$687 million in the first half of 2012. Similarly, Google Transparency Report reveals that the search engine giant flags around 10,000 websites as unsafe on a daily basis because of phishing and malware.

Sexual Abuse, Pedophiles, and Pornography

The Internet is not just flooded with illegal pornographic content, but is also full of sexual predators on a lookout for easy prey. There are several cases of pedophiles trapping children via chat and web cams, bullying them into meeting in person, and abusing them. Internet pornography is a major threat for the people who frequently keep on posting their photographs and videos over the Internet, since these can be misused and even posted on pornographic sites.

In 1998, the National Center for Missing & Exploited Children started the CyberTipline (1-800-843-5678) to help people report crimes against children. Since its inception, it has received more than 1.7 million reports of suspected child sexual exploitation. Furthermore, between 2004 and 2008, the law enforcement agencies working on Internet Crimes Against Children recorded a rise of 230 percent in the number of documented complaints of online enticement.

Cyberterrorism - A Threat to National Security

Several government websites contain important information, which is either uploaded over the Internet or stored in their database. These websites are vulnerable to security threats since many people try to break into security systems to access undisclosed matters of national importance. Almost every major terror group uses the Internet today, primarily as a propaganda tool and also as a means of communication. Cyber-terrorists can also bring down the infrastructure, which is more or less dependent on the Internet today, to spread panic in the world. While cyberterrorism is definitely a threat, criminal activities

(e.g. Internet extortion) and nuisance attacks (e.g. email bombing) are also rampant in the virtual world.

Ways to Ensure Internet Safety

Secure Your Network

Taking into account how vulnerable we are to cybercrimes, having strong firewall protection for the network is a must today. In case you want to secure your network for your home PC, you need a basic firewall, anti-virus software, anti-spyware software, and a robust password in case of wireless connections. In case you have a medium business, you would need a strong firewall and all the previously mentioned parameters with the addition of physical security and a network analyzer. In case of large businesses, you would require stronger Internet security software and security fencing in addition to the network analyzers.

Be Responsible

Internet safety is not just about making your network secure, but is also about being responsible when you are online. You should not upload your pictures and videos on social networking sites that do not provide strong privacy settings. Make sure that you go through the website's privacy policy and also resort to the most stringent privacy settings for your social networking profile. Do not accept friends/chat request from strangers. Anonymous surfing is yet another safety measure that--though simple--can help you secure your Internet.

Make Internet Child-safe

It is safe to educate your children about the possible dangers of the Internet and supervise their online activities for a while, but your children might get a wrong impression if they realize that you are spying on their online activities. This is where cyber security software and hardware come to you rescue. It is possible to make Internet child-safe by using software which allows you block websites which are not ideal for children. An even better option is to have a healthy relationship with your children. It will help you discuss the dos and don'ts of the Internet with them, without sounding preachy.

Internet safety or Internet security is an important issue that needs to be dealt with for safeguarding the security and privacy over the World Wide Web. With Internet security threats, like hacking, phishing, spyware and virus attacks, identity thefts, cyberbullying, child pornography, etc., becoming commonplace, it is high time you resort to smart-surfing and protect your computer and your data online.

II. Put 5 questions to the text.

Example: What is one of the major threats as far as Internet safety is concerned?

КОНТРОЛЬНА РОБОТА №3
ВАРІАНТ №7

I. Translate this text in writing:

Text **DON'T BE A STRANGER.**

Social media keep old friends close, but the Web used to be for strangers
The Internet of 2006 was not much different than it is today, mainly less: a bit slower, sparser, less open for business, like your hometown before the strip mall got put in. It was on this Internet that I met my best friend, Austin (not his real name). I was taking some time off from college in Portland, Oregon and had become an active member of a Portland-based online DIY community called Urban Honking. Urban Honking featured a stable of blogs about studiedly eclectic subjects like rap music, vegan cooking, and science fiction, but I spent most of my time on the message board, where a few dozen mostly twenty-somethings traded music recommendations and outlandish project ideas. At the time I was making stupid comedy videos and I'd share them with Urban Honking as I finished them. Austin was also an active Urban Honking poster, and a few months after I joined he sent me an email from his Yahoo! Mail account. Subscribe to TNI magazine for $2 and get TNI Vol. 13: <3 today.

"Hey dude," Austin wrote, "I saw you on the UrHo message board and wanted to get in touch because I like being funny and making videos." When we met up for a drink I found that Austin was about a foot taller and half a dozen years older than me, rail-thin, heavily-bearded and married. Standing next to each other, we formed the punch-line of a visual gag. We hit it off instantly, and he remains one of my closest friends—a friendship which, now that I live across the country in New York, largely exists through Gchat and email.

When someone asks me how I know someone and I say "the Internet," there is often a subtle pause, as if I had revealed we'd met through a benign but vaguely kinky hobby, like glassblowing class, maybe. The first generation of digital natives are coming of age, but two strangers meeting online is still suspicious (with the exception of dating sites, whose bare utility has blunted most stigma). What's more, online venues that encourage strangers to form lasting friendships are dying out. Forums and emailing are being replaced by Facebook, which was built on the premise that people would rather carefully populate their online life with just a handful of "real" friends and shut out all the trolls, stalkers, and scammers. Now that distrust of online strangers is embedded in the code of our most popular social network, it is becoming increasingly unlikely for people to interact with anyone online they don't already know.

Some might be relieved. The online stranger is the great boogeyman of the information age; in the mid-2000s, media reports might have had you believe that MySpace was essentially an easily-searchable catalogue of fresh victims for serial killers, rapists, cyberstalkers, and Tila Tequila. These days, we're warned of "catfish" con artists who create attractive fake online personae and begin relationships with strangers to satisfy some sociopathic emotional need. The term comes from the documentary Catfish and the new MTV reality show of the same name.

The technopanics over online strangers haunting the early social web were propelled by straight-up fear of unknown technology. Catfish shows that the fear hasn't vanished with social media's ubiquity, it's just become as banal as the technology itself. Each episode follows squirrelly millennial filmmaker Nev Schulman as he introduces someone in real life to a close friend or lover they've only known online. Things usually don't turn out as well as it did for me and Austin, to say the least. In the first episode, peppy Arkansas college student Sunny gushes to Schulman over her longtime Internet boyfriend, a male model and medical student named Jamison. They have never met or even video-chatted, but Sunny knows Jamison is The One.

"The chance of us meeting, and the connection we built is really something—once in a lifetime," Sunny says. But when Schulman calls Jamison's phone to get his side of the story it's answered by someone who sounds like a middle-schooler pretending to be ten years older to buy beer at a gas station. Each detail of Jamison's biography is more improbable than the last. The only surprise when Sunny and Schulman arrive at Jamison's house in Alabama and learn that the chiseled male model she fell for is actually a sun-deprived young woman named Chelsea, is how completely remorseless Chelsea is about the whole thing.

But Catfish isn't a cautionary tale about normal people being victimized by weirdos they meet on the Internet. By lowering the stakes from death or financial ruin to heartbreak, Catfish can blame the victim as well as the perpetrator. The hoaxes are so stupidly obvious from the beginning that it's impossible to feel empathy for targets like Sunny. Who's really "worse" in this situation: The lonely woman who pretends, poorly, to be a male model on the Internet, or the one who plows time and energy into such an obvious fraud? Catfish indicts the entire practice of online friendship as a depressing massively multiplayer online game in which the deranged entertain the deluded. Catfish is Jerry Springer for the social media age. Like the sad, bickering subjects of Springer's show, Sunny and Jamison deserve each other.

Catfish has struck such a nerve because it combines old fears of Internet strangers with newer anxieties about the authenticity of online friendship. Recently, an army of op-ed writers and best-selling authors have argued that social media is degrading our real-life relationships. “Friendship is devolving from a relationship to a feeling,” wrote the cultural critic William Deresiewicz in 2009, “from something people share to something each of us hugs privately to ourselves in the loneliness of our electronic caves.” Catfish‘s excruciating climaxes dramatize this argument. We see what happens when people like Sunny treat online friendships as if they’re “real,” and the end result is not pretty, literally.Don’t miss Adrian moderating the <3 release panel “What Was The Date?” on Feb. 25

Today’s skepticism of online relationships would have dismayed the early theorists of the Internet. For them, the ability to communicate with anyone, anywhere, from the privacy of our “electronic caves” was a boon to human interaction. The computer scientist J.C.R. Licklider breathlessly foretold the Internet in a 1968 paper with Robert W. Taylor, “The Computer as a Communication Device”: He imagined that communication in the future would take place over a network of loosely-linked “online interactive communities.” But he also predicted that “life will be happier for the on-line individual, because those with whom one interacts most strongly will be selected more by commonality of interests and goals than by accidents of proximity.” The ability to associate online with those we find most stimulating would lead to truer bonds than real world relationships determined by arbitrary variables of proximity and social class.

Obviously, we do not today live in a wired utopia where, as Licklider predicted, “unemployment would disappear from the face of the earth forever,” since everyone would have a job maintaining the massive network. But if Licklider was too seduced by the transformative power of the Internet, today’s social media naysayers are as well. To the Death of Friendship crowd, the Internet is a poison goo that corrodes the bonds of true friendship through Facebook’s trivial status updates and boring pictures of pets and kids. While good at selling books and making compelling reality television, this argument misses the huge variety of experience available online. Keener critics understand that our discontent with Facebook can be traced back to the specific values that inform that site. “Everything in it is reduced to the size of its founder,” Zadie Smith writes of Facebook, “Poking, because that’s what shy boys do to girls they’re scared to talk to. Preoccupied with personal trivia, because Mark Zuckerberg thinks the exchange of personal trivia is what ‘friendship’ is.”

II. Put 5 questions to the text.

Example: What is the online stranger?

КОНТРОЛЬНА РОБОТА №3
ВАРІАНТ №8

I. Translate this text in writing:

Text **DON'T BE A STRANGER (continued).**

Instead of asking, "is Facebook making us lonely?" and aimlessly pondering Big Issues of narcissism, social disintegration, and happiness metrics, as in a recent Atlantic cover story, we should ask: What exactly is it about Facebook that makes people ask if it's making us lonely? The answer is in Mark Zuckerberg's mind; not Mark Zuckerberg the awkward college student, where Zadie Smith finds it, but Mark Zuckerberg the programmer. Everything wrong with Facebook, from its ham-fisted approach to privacy, to the underwhelming quality of Facebook friendship, stems from the fact that Facebook models human relations on what Mark Zuckerberg calls "The social graph."

"The idea," he's said, "is that if you mapped out all the connections between people and the things they care about, it would form a graph that connects everyone together."

Facebook kills Lidlicker's dream of fluid "on-line interactive communities" by fixing us on the social graph as surely as our asses rest in our chairs in the real world. The social graph is human relationships modeled according to computer logic. There can be no unknowns on the social graph. In programming, an unknown value is also known as "garbage." So Facebook requires real names and real identities. "I think anonymity on the Internet has to go away," explained Randi Zuckerberg, Mark's sister and Facebook's former marketing director. No anonymity means no strangers. Catfish wouldn't happen in Zuckerberg's ideal Internet, but neither would mine and Austin's serendipitous friendship. Friendship on Mark Zuckerberg's Internet is reduced to trading pokes and likes with co-workers or old high school buddies.

"A computer is not really like us," wrote Ellen Ullman, a decade before the age of social media. "It is a projection of a very small part of ourselves; that portion devoted to logic, order, rule and clarity." These are not the values associated with a fulfilling friendship.

But what if a social network operated according to a logic as different from computer logic as an underground punk club is from a computer lab? Once upon a time this social network did exist, and it was called Makeoutclub.com. Nobody much talks about Makeoutclub.com these days, because in technology the only things that remain after the latest revolution changes everything all over again is

the heroic myth of the champion's victory (Facebook) and the loser's cautionary tale (MySpace). Makoutclub didn't win or lose; it barely played the game.

Makeoutclub was founded in 2000, four years before Facebook, and is sometimes referred to as the world's first social network. It sprung from a different sort of DIY culture than the feel-good Northwest indie vibes of Urban Honking. Makeoutclub was populated by lonely emo and punk kids, founded by a neck-tattooed entrepreneur named Gibby Miller, out of his bedroom in Boston.

The warnings of social disintegration and virtual imprisonment sounded by today's social media skeptics would have seemed absurd to the kids of Makeoutclub. They applied for their account and filled out the rudimentary profile in order to expand their identities beyond lonely real lives in disintegrating suburban sprawl and failing factory towns. Makeoutclub was electrified by the simultaneous realization of thousands of weirdos that they weren't alone.

With Makeoutclub, journalist Andy Greenwald writes in his book Nothing Feels Good: Punk Rock, Teenagers, and Emo,

Kids in one-parking-lot towns had access not only to style (e.g., black, black glasses), but also what books, ideas, trends, and beliefs were worth buzzing about in the big cities. If, in the past, one wondered how the one-stoplight town in Kansas had somehow birthed a true-blue Smiths fan, now subculture was the same everywhere. Outcasts had a secret hideout. Makeoutclub.com was one-stop shopping for self-makers.

As the name would suggest, Makeoutclub was also an excellent place to hook up. But because it wasn't explicitly a dating service, courtship on Makeoutclub was free of OKCupid's mechanical numbness. Sex and love were natural fixations for a community of thousands of horny young people, not a programming challenge to be solved with sophisticated algorithms.

About three years before I met my funny friend Austin on Urban Honking in Portland, Austin met his wife on Makeoutclub.com. Austin told me he joined in 2001 when he was 21 years old, "because it was easy to do and increased my chance of meeting a cute girl I could date." You could search users by location, which made it easy to find someone in your area. (On Facebook, it's impossible to search for people without being guided to those you are most likely to already know; results are filtered according to the number of mutual friends you have.)

Austin would randomly message interesting-seeming local women whenever he came back home from college and they'd go on dates that almost invariably ended in no making out. In the real world, Austin was awkward.

Makeoutclub brought people together with a Lickliderian common interest, but it didn't produce a Lickliderian utopia. It was messy; crews with names like "Team Vegan and "Team Elitist Fucks" battled on the message board, and creeps haunted profiles. But since anyone could try to be an intriguing stranger, the anonymity bred a productive recklessness. One night, around 2004, Austin was browsing Makeoutclub when he found his future wife. By this time, he'd graduated college and moved to Norway on a fellowship, where he fell into a period of intense loneliness. He'd taken again to messaging random women on Makeoutclub to talk to, and that night he messaged Dana, a Canadian who had caught his eye because she was wearing an eye patch in her profile picture. Subscribe to TNI magazine for $2 and get TNI Vol. 13: <3 today.

"I had recently made a random decision that if I met a girl with a patch over her eye, I would marry her," Austin told me. "I don't know why I made this decision, but at the time I was making lots of strange decisions." He explained this to Dana in his first message to her. They joked over instant messenger for a few days, but after a while their contact trailed off.

Months later, after Austin had moved from Norway to New York City, he received a surprising instant message from Dana. It turned out that Dana had meant to message another friend with a similar screenname to Austin's. They got to chatting again, and Dana said she'd soon be taking a trip to New York City to see the alt-cabaret group Rasputina play. Dana and Austin met up the night before she was supposed to return to Canada. They got along. Dana slept over at Austin's apartment that night and missed her flight. When Dana got back to Canada they kept in touch, and within a few weeks, Austin asked her to marry her. Today, they've been married for over eight years.

Dana and Austin's relationship, and mine and Austin's friendship, shows the Licklider dream was not as naïve as it appears now at first glance. If you look to online communities outside of Facebook, strangers are forging real and complex friendships, despite the complaints of op-ed writers. Even today, I've met some of my best friends on Twitter, which is infinitely better at connecting strangers than Facebook. Unlike the almost gothic obsession of Catfish's online lovers, these friendships aren't exclusively online—we meet up sometimes to talk about the Internet in real life. They are not carried out in a delusional swoon, or by trivial status updates.

These are not brilliant Wordsworth-and-Coleridge type soul-meldings, but they are not some shadow of a "real" friendship. Internet friendship yields a connection that is selfconsciously pointless and pointed at the same time: Out of all of the millions of bullshitters on the World Wide Web, we somehow found each other, liked each other enough to bullshit together, and built our own Fortress of Bullshit. The majority of my interactions with online friends is perpetuating some injoke so arcane that nobody remembers how it started or what it actually means. Perhaps that proves the op-ed writers' point, but this has been the pattern of my friendships since long before I first logged onto AOL, and I wouldn't have it any other way.

Makeoutclub isn't dead either, but it seems mired in nostalgia for its early days. This past December, Gibby Miller posted a picture he'd taken in 2000 to Makeoutclub's forums — it was the splash image for its first winter. It's a snowy picture of his Boston neighborhood twelve years ago, unremarkable except for the moment of time it represents.

"This picture more than any other brings me back to those days," Miller wrote in the forum. "All ages shows were off the hook, 'IRL' meetups were considered totally weird and meeting someone online was unheard of, almost everyone had white belts and dyed black Vulcan cuts."

At least the Vulcan cuts have gone out of style.

II. Put 5 questions to the text.
Example: When did Dana and Austin meet up?

КОНТРОЛЬНА РОБОТА №3
ВАРІАНТ №9

I. Translate this text in writing:

Text **SPAM + BLOGS = TROUBLE**

I am aware that spending a lot of time Googling yourself is kind of narcissistic, OK? But there are situations, I would argue, when it is efficiently – even forgivably – narcissistic. When I published a book last year, I wanted to know what, if anything, people were saying about it. Ego-surfing was the obvious way to do that. Which is how I stumbled across Some Title.

Some Title identified itself as a blog but obviously wasn't one. Here, reprinted in its entirety, is the paragraph from the site that mentioned me:

Show Disputed Vinland Map Was Made Half Century Before Columbus Trip Audio/Video Columbus: Secrets From The Grave quot;The Last Voyage of Columbus quot;: An Epic Tale Charles Mann's quot;1491 quot; (Audio
In orthodox bloggy style, the paragraph linked to another Web page. When I clicked on the link, I was confronted with more gibberish: "Below," it stated, "you will find some grave robbing in ventura california 1985 news that's relevant for today."

Blogs like Some Title are known as "splogs" – spam blogs. Like email spam, splogs use the most wonderful features of networked communication – its flexibility, easy access, and low cost – in the service of sleazy get-rich-quick schemes. But whereas email spammers try to induce recipients to buy products, sploggers and other Web spammers make most of their money by getting viewers to click on ads that run adjacent to their nonsensical text. Web page owners – the spammer, in this case – get paid by the advertiser every time someone clicks on an ad.

Some Title's creator had almost certainly assembled the site by using software that hops from Web page to Web page, automatically copying text that includes potential search terms. (My name and my book's title had been included incidentally, because they appeared in a review or blog that happened to contain keywords sought by the spammer.) Sploggers don't care if the resulting Web pages are garbled; the point is to churn them out chockablock with terms that people might use in search queries, leading them to visit the pages and click (ka-ching!) on the ads.

Just as the proliferation of email spam constantly threatens to inundate email providers, the explosion of blog spam is a besetting problem for the blog industry. Like most people who poke around the blogosphere, I had occasionally encountered splogs before. But over the months that I monitored the reaction to my book, they seemed to be rising in number. More and more of the blogs and Web sites that mentioned my book – or any other topic, for that matter – were spam. Some 56 percent of active English-language blogs are spam, according to a study released in May by Tim Finin, a researcher at the University of Maryland, Baltimore County, and two of his students. "The blogosphere is growing fast," Finin says. "But the splogosphere is now growing faster."

To Jason Goldman, product manager for Google's Blogger hosting service, "the ever-increasing number of splogs is a significant problem that we have to combat." No search engine wants users looking for information about, say, auto repair to click on a promising link and end up on a page filled with jabberwocky or a collection of advertisements. Nor does any blog host want to waste its

resources and trash its reputation by providing a home to spammers. A recent survey by Mitesh Vasa, a Virginia-based software engineer and splog researcher, found that in December 2005, Blogger was hosting more than 100,000 sploggers. (Many of these are likely pseudonyms for the same people.)

Google, Goldman promises, is paying serious attention to the problem. It should be: The pay-per-click advertising that accounts for most of Google's income (and, increasingly, for the incomes of Yahoo and MSN Search, the two other big search engines) has become an irresistible magnet for hucksters, con artists, and chiselers. "The three main search engines are gateways to a huge percentage of the US and world economy," says Anil Dash, a vice president of the blog-hosting company Six Apart. "If your Web site appears high up on their results, thousands or millions of people will go to it." If even a small fraction of those people click on the ads on that site, "you're going to make a lot of money" – and sploggers are going after it.

Because the ad money is effectively available only to Web sites that appear in the first page or two of search results, spammers devote enormous efforts to gaming Google, Yahoo, and their ilk. Search engines rank Web sites in large part by counting the number of other sites that link to them, assigning higher placement in results to sites popular enough to be referred to by many others. To mimic this popularity, spammers create bogus networks of interconnected sites called link farms. Blogs – most of which are in essence little more than collections of links with commentary – are particularly useful elements in them. The result, Dash says, "is what you'd expect: The blogosphere is increasingly polluted by spam."

The mess may have consequences beyond the blogosphere, though. Blogs are the leading edge of what is often called Web 2.0, the vision of the Internet as a bottom-up, communal platform for data of all sorts that is generated and continually updated by its users: the image-sharing sites Flickr and YouTube, the social bookmarking destination del.icio.us, the collaborative online encyclopedia Wikipedia, the user-generated Slashdot rival digg, and publicly viewable online calendars like Kiko and CalendarHub. Unfortunately, the very openness and ease of use that make these Web 2.0 sites popular will inevitably make them perfect targets for spammers, says Matt Mullenweg, developer of the popular WordPress blogging system. "Extreme vulnerability to spam," he says, is a defining characteristic of Web 2.0, and splogs are its first manifestation.

People in the industry disagree about how to beat back spam, or whether it can even be done. But there's no dispute that if the blogosphere and the rest of Web 2.0 can't find a way to stop the sleazeballs who are enveloping the Net in a haze

of babble and cheesy marketing, then the best features of Web 2.0 will be turned off, and it will go the way of Usenet, which was driven to desuetude by spam.

Some Title, the splog that commandeered my name, was created by Dan Goggins, the proud possessor of a 2005 master's degree in computer science from Brigham Young University. Working out of his home in a leafy subdivision in Springville, Utah, Goggins, his BYU friend and partner, John Jonas, and their handful of employees operate "a few thousand" splogs. "It's not that many," Goggins says modestly. "Some people have a lot of sites." Trolling the Net, I came across a PowerPoint presentation for a kind of spammers' conference that details some of the earnings of the Goggins-Jonas partnership. Between August and October of 2005, they made at least $71,136.89.

II. Put 5 questions to the text.
Example: What features of networked communication do the splogs use?

КОНТРОЛЬНА РОБОТА №3
ВАРІАНТ №10

I. Translate this text in writing:

Text **VIRUSES ARE GOOD FOR YOU**

Spawn of the devil, computer viruses may help us realize the full potential of the Net.
What scares you most about getting that virus?

Is it the prospect of witnessing your system's gradual decay, one nagging symptom following another until one day the whole thing comes to a halt? Is it the self-recrimination, all the useless dwelling on how much easier things would have been if only you'd protected yourself, if only you'd been more careful about whom you associated with?

Or is it not, in fact, something deeper? Could it be that what scares you most about the virus is not any particular effect it might have, but simply its assertive, alien presence, its intrusive otherness? Inserting itself into a complicated choreography of subsystems all designed to serve your needs and carry out your will, the virus hews to its own agenda of survival and reproduction. Its oblivious self-interest violates the unity of purpose that defines your system as yours. The virus just isn't, well, you. Doesn't that scare you?

And does it really matter whether the virus in question is a biological or an electronic one? It should, of course. The analogy that gives computer viruses their name is apt enough to make comparing bioviruses and their digital analogs an interesting proposition, but it falls short in one key respect. Simply put, the only way to fully understand the phenomenon of autonomously reproducing computer programs is to take into account their one essential difference from organic life forms: they are products not of nature but of culture, brought forth not by the blind workings of a universe indifferent to our aims, but by the conscious effort of human beings like ourselves.

Why then, after a decade of coexistence with computer viruses, does our default response to them remain a mix of bafflement and dread? Can it be that we somehow refuse to recognize in them the traces of our fellow earthlings' shaping hands and minds? And if we could shake those hands and get acquainted with those minds, would their creations scare us any less?

These are not idle questions. Overcoming our fear of computer viruses may be the most important step we can take toward the future of information processing. Someday the Net will be the summation of the world's total computing resources. All computers will link up into a chaotic digital soup in which everything is connected - indirectly or directly - to everything else. This coming Net of distributed resources will be tremendously powerful, and tremendously hard to harness because of its decentralized nature. It will be an ecology of computing machines, and managing it will require an ecological approach.

Many of the most promising visions of how to coordinate the far-flung communication and computing cycles of this emerging platform converge on a controversial solution: the use of self-replicators that roam the Net. Free-ranging, self-replicating programs, autonomous Net agents, digital organisms - whatever they are called, there's an old fashion word for them: computer viruses.

Today three very different groups of heretics are creating computer viruses. They have almost nothing to do with each other. There are scientists interested in the abstract behaviors of self-replicating codes, there are developers interested in harnessing the power of self-replicating programs, and there are unnamed renegades of the virus-writing underground.

Although they share no common experience, all these heretics respect a computer virus for its irrepressible mobility, for the self-centered autonomy it wrests from a computer environment, and for the surprising agility with which it explores opportunities and possibilities. In short, virus enthusiasts relate to the virus as a fascinating and powerful life form, whether for the fertile creation of

yet more powerful digital devices, as an entity for study in itself, or, in the case of one renegade coder, for reckless individual expression.

Getting a buzz from the Vx

One computer virus writer in his early 20s lives on unemployment checks in a white, working-class exurb of New York City. He tends to spend a fair amount of his leisure time at the local videogame arcade playing Mortal Kombat II, and would prefer that you didn't know his real name. But don't let the slacker resume fool you: the only credential this expert needs is the pseudonym he goes by in the computer underground: Hellraiser.

Hellraiser is the founding member of the world-renowned virus-writers' group Phalcon/Skism. He is also creator of 40Hex, an electronic zine whose lucid programming tips, hair-raising samples of ready-to-run viral code, and trash-talking scene reports have done more to inspire the creation of viruses in this country than just about anything since Robert Morris Jr.'s spectacularly malfunctional worm nearly brought down the Internet.

And as if all this weren't enough, Hellraiser also comes equipped with the one accessory no self-respecting expert in this cantankerous field can do without - his very own pet definition of computer viruses. Unlike most such definitions, Hellraiser's is neither very technical nor very polemical, and he doesn't go out of his way to make it known. "Sure," he'll say, with a casual shrug, as if tossing you the most obvious fact in the world: "Viruses are the electronic form of graffiti."

Which would probably seem obvious to you too, if you had Hellraiser's personal history. For once upon his teenage prime, Hellraiser was also a hands-on expert in the more traditional forms of graffiti perfected by New York City youth in the 1980s. Going by the handle of Skism, he roamed the city streets and train yards with a can of spray paint at the ready and a Bronx-bred crew of fellow "writers" at his side, searching out the sweet spots in the transit system that would give his tag maximum exposure - the subway cars that carried his identity over the rails, the truck trailers that hauled it up and down the avenues, and the overpasses that announced it to the flow of travelers circulating underneath.

In other words, by the time Hellraiser went off to college and developed a serious interest in computers, he was already quite cozy with the notion of infiltrating other people's technology to spread a little of himself as far and wide as possible. So when he discovered one day that his PC had come down with a nasty little digital infection, his first thought was not, as is often customary, to

curse the "deviant hackers," "sociopaths," and "assholes" who had written the program, but to marvel at the possibilities this new infiltration technique had opened up. Street graffiti's ability to scatter tokens of one's identity across the landscape of an entire metropolis looked provincial in comparison. "With viruses," Hellraiser remembers thinking, "you could get your name around the world."

He was right. The program that had infected his own computer in late 1990, the so-called Jerusalem virus, had spread from Italy to Israel to North America before finally making its way into the pirated copy of the Norton Utilities that brought it to Hellraiser's hard drive. And though Jerusalem's author remained uncredited, other programmers from nearly every corner of the globe were pulling off feats of long-distance self-aggrandizement that dwarfed anything within the reach of America's spray-paint commandos. A kid who called himself Den Zuk had launched a virus that was flashing his handle on computer screens all over Europe, the US, and South America. Early speculation placed its origin in Venezuela, but the virus was eventually tracked to its true source in Bandung, Indonesia, when a researcher in Iceland guessed that some enigmatic characters in the source code were in fact a ham-radio call sign; they made contact with the call sign's registered operator, who immediately copped to his authorship of the program.

Equally far-ranging was the journey of the Joshi virus, which spread from India to parts of Africa and on to the rest of the world, popping up every January 5th to command computer users to type "Happy Birthday Joshi" if they wanted control of their systems back.

What impressed Hellraiser as much as the vast geographic distances covered by viruses, however, was their long range over time. After all, a painted graffiti tag would only last as long as it took to fade away or be painted over, but viruses, it seemed, might replicate forever in the wild. Indeed, the Jerusalem virus had been doing so for three years before Hellraiser encountered it, and four years later it remains one of the world's most commonly reported viruses. Likewise, Den Zuk is still reproducing on computers worldwide six years after it first left the island of Java; Joshi continues for the fifth year in a row to extort international birthday wishes. Dozens of other viruses from the US, Canada, Eastern Europe, Taiwan, Australia, Turkey, Malta, and other far-flung locales thrive globally (This despite that the antivirus industry spends tens of millions of dollars a year to eradicate them.) Bearing encoded bits of their authors' souls - clever jokes, crude graphics, friendly greetings, and, of course, occasionally, malicious intentions (though in fact the majority of viruses found in the wild are designed to do no damage) - viruses roam the earth in apparent perpetuity.

For Hellraiser, steeped as he was in graffiti culture's imperative to "get the name across," there was only one possible response to this new technology of self-projection: he had to get in on the action. But how? Virus writing wasn't exactly a standard subject in computer-science courses, and even the computer underground - with its loose-knit network of bulletin boards and e-zines proffering instruction in the illicit arts of hacking and phone phreaking - wasn't the most dependable source of virus lore. Occasionally, a hack and phreak board might offer a small collection of cryptic viral source code for brave souls to experiment with, but as far as Hellraiser knew, the only system exclusively devoted to viruses at the time was a place called the Virus Exchange, operating out of what was then the world's epicenter of virus production: post-Communist Bulgaria, where the Cold War's endgame had left a lot of overtrained programmers with time on their hands and anarchy on their minds.

II. Put 5 questions to the text.

Example: Who is the founding member of the world-renowned virus-writers' group Phalcon/Skism?

Література

1. S. G. Nash, A History of Scientific Computing (1990);

2. D. I. A. Cohen, Introduction to Computer Theory (2d ed. 1996);

3. P. Norton, Peter Norton's Introduction to Computers (2d ed. 1996);

4. A. W. Biermann, Great Ideas in Computer Science: A Gentle Introduction (2d ed. 1997);

5. R. L. Oakman, The Computer Triangle: Hardware, Software, People (2d ed. 1997);

6. R. Maran, Computers Simplified (4th ed. 1998);

7. A. S. Tanenbaum and J. R. Goodman. Structured Computer Organization (4th ed. 1998);

8. Clark, D. Computers at Risk: Safe Computing in the Information Age, National Research Council, National Academy Press, 1990;

9. Pressman, R. S. & Herron, R. Software Shock: The Danger and the Opportunity. Dorsett House, 1991.