**COMPUTER SECURITY AND RISKS**

**BASIC COMPUTER SECURITY CONCEPTS**

**Read the following words and word combinations and use them for understanding and translation of the text:**

**confidentiality** - конфиденциальность

**integrity** - целостность

**availability** - доступность

**to pertain to** - иметь отношение к...

**authentication** - аутентификация, подлинность

**authorization** - авторизация

**nonrepudiation** - реотрицаемость, строгое выполнение обязательств

**to corrupt** – повреждать, искажать

**tampering** - взлом

**password** - пароль

**to refute** - опровергать

**trustworthy** - заслуживающий доверия

**intruder** - злоумышленник

**weak link** - слабое звено

**innocuous** - безвредный

**break-in** - проникновение в систему

**to compromise** - раскрывать

**denial-of-service** - отказ в обслуживании

**Computer security** (also known as **cybersecurity** or **IT security**) is information security as applied to computing devices such as computers and smartphones, as well as computer networks such as private and public networks, including the Internet as a whole.

There are many characterizations of computer security. Information technology security is defined in a document created by the European Community, which has gained some recent international acceptance. The document defines information technology (IT) security to include the following:

• Confidentiality. Prevention of unauthorized disclosure of information.

• Integrity. Prevention of unauthorized modification of information.

• Availability. Prevention of unauthorized withholding of information or resources.

Availability pertains to both information and resources, such as computer systems themselves. Confidentiality and integrity pertain only to information itself. Concepts relating to the people who use that information are authentication, authorization, and nonrepudiation.

When information is read or copied by someone not authorized to do so, the result is known as loss of **confidentiality**. For some types of information, confidentiality is a very important attribute. Examples include research data, medical and insurance records, new product specifications, and corporate investment strategies. In some locations, there may be a legal obligation to protect the privacy of individuals. This is particularly true for banks and loan companies; debt collectors; businesses that extend credit to their customers or issue credit cards; hospitals, doctors’ offices, and medical testing laboratories; individuals or agencies that offer services such as psychological counseling or drug treatment; and agencies that collect taxes.

Information can be corrupted when it is available on an insecure network. When information is modified in unexpected ways, the result is known as loss of **integrity**. This means that unauthorized changes are made to information, whether by human error or intentional tampering. Integrity is particularly important for critical safety and financial data used for activities such as electronic funds transfers, air traffic control, and financial accounting.

Information can be erased or become inaccessible, resulting in loss of **availability**. This means that people who are authorized to get information cannot get what they need. Availability is often the most important attribute in service-oriented businesses that depend on information (for example, airline schedules and online inventory systems).

Availability of the network itself is important to anyone whose business or education relies on a network connection. When users cannot access the network or specific services provided on the network, they experience a denial-of-service.

To make information available to those who need it and who can be trusted with it, organizations use **authentication and authorization**. Authentication is proving that a user is the person he or she claims to be. That proof may involve something the user knows (such as a password), something the user has (such as a “smartcard”), or something about the user that proves the person’s identity (such as a fingerprint). Authorization is the act of determining whether a particular user (or computer system) has the right to carry out a certain activity, such as reading a file or running a program.

Authentication and authorization go hand in hand. Users must be authenticated before carrying out the activity they are authorized to perform. Security is strong when the means of authentication cannot later be refuted — the user cannot later deny that he or she performed the activity. This is known as **nonrepudiation**.

The Internet users want to be assured that

* they can trust the information they use
* the information they are responsible for will be shared only in the manner that they expect
* the information will be available when they need it
* the systems they use will process information in a timely and trustworthy manner

It is remarkably easy to gain unauthorized access to information in an insecure networked environment, and it is hard to catch the intruders. Even if users have nothing stored on their computer that they consider important, that computer can be a “weak link,” allowing unauthorized access to the organization’s systems and information.

Seemingly innocuous information can expose a computer system to compromise. Information that intruders find useful includes which hardware and software are being used, system configuration, type of network connections, phone numbers, and access and authentication procedures. Security-related information can enable unauthorized individuals to access important files and programs, thus compromising the security of the system. Examples of important information are passwords, access control files and keys, personnel information, and encryption algorithms.

The consequences of a break-in cover a broad range of possibilities: a minor loss of time in recovering from the problem, a decrease in productivity, a significant loss of money or staff-hours, a devastating loss of credibility or market opportunity, a business no longer able to compete, legal liability, and the loss of life. Individuals may find that their credit card, medical, and other private information has been compromised.

**Assignments**

**1. Translate the sentences from the texts into Russian in writing paying attention to the underlined words and phrases:**

1. Information can be corrupted when it is available on an insecure network.
2. When information is modified in unexpected ways, the result is known as loss of integrity. This means that unauthorized changes are made to information, whether by human error or intentional tampering**.**
3. Availability is often the most important attribute in service-oriented businesses that depend on information.
4. When users cannot access the network or specific services provided on the network, they experience a denial of service.
5. Security is strong when the means of authentication cannot laterbe refuted - the user cannot later deny that he or she performed the activity.
6. It is remarkably easy to gain unauthorized access to information in an insecure networked environment, and it is hard to catch the intruders.

**2. Answer the following questions:**

1. In what spheres of human activity does availability play an essential role? Why?
2. When will security be the strongest?
3. Which concept is the most remarkable for the provision of overall security?
4. What can be the consequences of an unauthorized break-in?
5. How can intruders benefit from the access to innocuous information?
6. Is there a principal difference between authorization and authentication?

**3. Translate into English:**

Под информационной безопасностью понимается за­щищенность информации и поддерживающей ее инфра­структуры от любых случайных или злонамеренных воз­действий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам или поддержи­вающей инфраструктуре.

Цель информационной безопасности - обезопасить ценности системы, защитить и гарантировать точность и целостность информации и минимизировать разрушения, которые могут иметь место, если информация будет моди­фицирована или разрушена.

На практике важнейшими являются три аспекта ин­формационной безопасности:

1. Доступность (возможность за разумное время полу­чить требуемую информационную услугу);

2. Целостность (ее защищенность от разрушения и не­санкционированного изменения);

3. Конфиденциальность (защита от несанкциониро­ванного прочтения).

**4. Give the summary of the text using the key terms.**

**TYPES OF INCIDENTS**

**Read the following words and word combinations and use them for understanding and translation of the text:**

**threat** - угроза

**violation** - нарушение

**disruption** - прерывание

**usurpation** — захват, неправомерное присвоение

**ubiquitous** - повсеместный

**snooping** - перехват

**wiretapping** — перехват при подключении к линии связи

**man-in-the-middle attack** — атака через посредника

**recipient** - получатель

**intermediary** - посредник

**masquerading** — выдача себя за другое лицо

**spoofing** - подмена

**to lure** - заманивать

**repudiation** - опровержение

**pending** - отложенный

**probe** - зонд

**packet sniffer** — перехватчик пакетов

**downtime** — нерабочее время, простой

**Threats**

A threat is a potential violation of security. The violation need not actually occur for there to be a threat. The fact that the violation might occur means that those actions that could cause it to occur must be guarded against (or prepared for). Those actions are called attacks.

Threats can be divided into four broad classes: disclosure, or unauthorized access to information; deception, or acceptance of false data; disruption, or interruption or prevention of correct operation; and usurpation, or unauthorized control of some part of a system. These four broad classes encompass many common threats. Since the threats are ubiquitous, an introductory discussion of each one will present issues that recur throughout the study of computer security.

**Snooping,** the unauthorized interception of information, is a form of disclosure. It is passive, suggesting simply that some entity is listening to (or reading) communications or browsing through files or system information. Wiretapping, or passive wiretapping, is a form of snooping in which a network is monitored.

**Modification or alteration**, an unauthorized change of information. Active wiretapping is a form of modification in which data moving across a network is altered; the term "active" distinguishes it from snooping ("passive" wiretapping). An example is the man-in-the-middle attack, in which an intruder reads messages from the sender and sends (possibly modified) versions to the recipient, in hopes that the recipient and sender will not realize the presence of the intermediary.

**Masquerading or spoofing**, an impersonation of one entity by another. It lures a victim into believing that the entity with which it is communicating is a different entity. This may be a passive attack (in which the user does not attempt to authenticate the recipient, but merely accesses it), but it is usually an active attack (in which the masquerader issues responses to mislead the user about its identity). It is often used to usurp control of a system by an attacker impersonating an authorized manager or controller.

**Repudiation of origin,** a false denial that an entity sent (or created) something. Suppose a customer sends a letter to a vendor agreeing to pay a large amount of money for a product. The vendor ships the product and then demands payment. The customer denies having ordered the product and by law is therefore entitled to keep the unsolicited shipment without payment. The customer has repudiated the origin of the letter. If the vendor cannot prove that the letter came from the customer, the attack succeeds.

**Delay**, a temporary inhibition of a service. Typically, delivery of a message or service requires some time *t*; if an attacker can force the delivery to take more than time *t*, the attacker has successfully delayed delivery. This requires manipulation of system control structures, such as network components or server components, and hence is a form of usurpation.

**Denial-of-service**

The goal of denial-of-service attacks is not to gain unauthorized access to machines or data, but to prevent legitimate users of a service from using it. A denial-of-service attack can come in many forms. Attackers may "flood" a network with large volumes of data or deliberately consume a scarce or limited resource, such as process control blocks or pending network connections. They may also disrupt physical components of the network or manipulate data in transit, including encrypted data.

**Attacks**

An attempt to breach system security may not be deliberate; it may be the product of environmental characteristics rather than specific actions of an attacker. Incidents can be broadly classified into several kinds: the probe, scan, account compromise, root compromise, packet sniffer, denial of service, exploitation of trust, malicious code, and Internet infrastructure attacks.

**Probe**

A probe is characterized by unusual attempts to gain access to a system or to discover information about the system. Probing is the electronic equivalent of testing doorknobs to find an unlocked door for easy entry. Probes are sometimes followed by a more serious security event, but they are often the result of curiosity or confusion.

**Scan**

A scan is simply a large number of probes done using an automated tool. Scans can sometimes be the result of a misconfiguration or other error, but they are often a prelude to a more directed attack on systems that the intruder has found to be vulnerable.

**Account compromise**

An account compromise is the unauthorized use of a computer account by someone other than the account owner, without involving system-level or root-level privileges (privileges a system administrator or network manager has). An account compromise might expose the victim to serious data loss, data theft, or theft of services.

**Root compromise**

A root compromise is similar to an account compromise, except that the account that has been compromised has special privileges on the system. Intruders who succeed in a root compromise can do just about anything on the victim’s system, including run their own programs, change how the system works, and hide traces of their intrusion.

**Packet sniffer**

A packet sniffer is a program that captures data from information packets as they travel over the network. That data may include user names, passwords, and proprietary information that travels over the network in clear text. With perhaps hundreds or thousands of passwords captured by the sniffer, intruders can launch widespread attacks on systems.

**Exploitation of trust**

Computers on networks often have trust relationships with one another. For example, before executing some commands, the computer checks a set of files that specify which other computers on the network are permitted to use those commands. If attackers can forge their identity, appearing to be using the trusted computer, they may be able to gain unauthorized access to other computers.

**Malicious code**

Malicious code is a general term for programs that, when executed, would cause undesired results on a system. Users of the system usually are not aware of the program until they discover the damage. Malicious code includes Trojan horses, viruses, and worms. Trojan horses and viruses are usually hidden in legitimate programs or files that attackers have altered to do more than what is expected. Worms are self-replicating programs that spread with no human intervention after they are started. Viruses are also self-replicating programs, but usually require some action on the part of the user to spread inadvertently to other programs or systems. These sorts of programs can lead to serious data loss, downtime, denial-of-service, and other types of security incidents.

**Internet infrastructure attacks**

These rare but serious attacks involve key components of the Internet infrastructure rather than specific systems on the Internet. Examples are network name servers, network access providers, and large archive sites on which many users depend. Widespread automated attacks can also threaten the infrastructure. Infrastructure attacks affect a large portion of the Internet and can seriously hinder the day-to-day operation of many sites.

**Assignments**

**1. Translate the sentences from the texts into Russian in writing paying attention to the underlined words and phrases:**

1. The fact that the violation might occur means that those actions that could cause it to occur must be guarded against (or prepared for).
2. Threats can be divided into four broad classes: disclosure, or unauthorized access to information; deception, or acceptance of false data; disruption, or interruption or prevention of correct operation; and usurpation, or unauthorized control of some part of a system.
3. Active wiretapping is a form of modification in which data moving across a network is altered; the term "active" distinguishes it from snooping ("passive" wiretapping).
4. Masquerading or spoofing is often used to usurp control of a system by an attacker impersonating an authorized manager or controller.
5. Attackers may "flood" a network with large volumes of data or deliberately consume a scarce or limited resource, such as process control blocks or pending network connections.
6. Scans can sometimes be the result of a misconfiguration or other error, but they are often a prelude to a more directed attack on systems that the intruder has found to be vulnerable.
7. An account compromise is the unauthorized use of a computer account by someone other than the account owner, without involving system-level or root-level privileges (privileges a system administrator or network manager has).
8. A packet sniffer is a program that captures data from information packets as they travel over the network. That data may include user names, passwords, and proprietary information that travels over the network in clear text.

**2. Answer the following questions:**

1. What is the principal difference between threats and attacks?
2. What are the four classes that encompass common threats?
3. What is the difference between passive and active wiretapping?
4. How do various types of denial-of-service attacks work?
5. Can the breaches of the system security be unintentional?
6. What are the consequences of a malicious code execution?

**3. Translate into English:**

Для подготовки и проведения атак могут использо­ваться либо специально разработанные для этих целей программные средства, либо легальные программы «мир­ного» назначения. Так, последний пример показывает, как легальная программа ping, которая создавалась в качестве инструмента диагностики сети, может быть применена для подготовки атаки. При проведении атак злоумышленнику важно не только добиться своей цели, заключающейся в причинении ущерба атакуемому объекту, но и уничтожить все следы своего участия в этом. Одним из основных прие­мов, используемых злоумышленниками для «заметания следов», является подмена содержимого пакетов (spoofing). В частности, для сокрытия места нахождения источника вредительских пакетов (например, при атаке отказа в об­служивании) злоумышленник изменяет значение поля ад­реса отправителя в заголовках пакетов. Поскольку адрес отправителя генерируется автоматически системным про­граммным обеспечением, злоумышленник вносит измене­ния в соответствующие программные модули так, чтобы они давали ему возможность отправлять со своего компью­тера пакеты с любыми IP-адресами.

**4. Give the summary of the text using the key terms.**

**IMPROVING SECURITY**

**Read the following words and word combinations and use them for understanding and translation of the text:**

**vulnerability** - уязвимость

**vigilance** - бдительность

**dissemination** - распределение

**to retrieve information** – извлекать информацию

**encryption** - шифрование

**decryption** - дешифровка

**patch** — исправление уязвимости

**alert** - тревога

**log** — журнал регистрации событий

**to install** - устанавливать

**gateway** - шлюз

**paging** — страничная организация памяти

**plaintext** — незашифрованный текст

**ciphertext** — зашифрованный текст

**confidentiality** - секретность

**checksum** — контрольная сумма

In the face of the vulnerabilities and incident trends discussed above, a robust defense requires a flexible strategy that allows adaptation to the changing environment, well-defined policies and procedures, the use of robust tools, and constant vigilance.

**Security policy**

Factors that contribute to the success of a security policy include management commitment, technological support for enforcing the policy, effective dissemination of the policy, and the security awareness of all users. Management assigns responsibility for security, provides training for security personnel, and allocates funds to security. Technological support for the security policy moves some responsibility for enforcement from individuals to technology. The result is an automatic and consistent enforcement of policies, such as those for access and authentication.

**Security-related procedures**

Procedures are specific steps to follow that are based on the computer security policy. Procedures address such topics as retrieving programs from the network, connecting to the site’s system from home or while traveling, using encryption, authentication for issuing accounts, configuration, and monitoring.

**Security practices**

System administration practices play a key role in network security. Checklists and general advice on good security practices are readily available. Below are examples of commonly recommended practices:

* Ensure all accounts have a password and that the passwords are difficult to guess. A one-time password system is preferable.
* Use tools such as MD5 checksums, a strong cryptographic technique, to ensure the integrity of system software on a regular basis.
* Use secure programming techniques when writing software.
* Be vigilant in network use and configuration, making changes as vulnerabilities become known.
* Regularly check with vendors for the latest available fixes, and keep systems current with upgrades and patches.
* Regularly check online security archives, such as those maintained by incident response teams, for security alerts and technical advice.
* Audit systems and networks, and regularly check logs. Many sites that suffer computer security incidents report that insufficient audit data is collected, so detecting and tracing an intrusion is difficult.

**Security technology**

A variety of technologies have been developed to help organizations secure their systems and information against intruders. These technologies help protect systems and information against attacks, detect unusual or suspicious activities, and respond to events that affect security.

**One-time passwords.** Intruders often install packet sniffers to capture passwords as they traverse networks during remote login processes. Therefore, all passwords should at least be encrypted as they traverse networks. A better solution is to use one-time passwords. These passwords are never repeated and are valid only for a specific user during the period that each is displayed. In addition, users are often limited to one successful use of any given password. One-time password technologies significantly reduce unauthorized entry at gateways requiring an initial password.

**Firewalls**. Intruders often attempt to gain access to networked systems by pretending to initiate connections from trusted hosts. They squash the emissions of the genuine host using a denial-of-service attack and then attempt to connect to a target system using the address of the genuine host. To counter these address-spoofing attacks and enforce limitations on authorized connections into the organization’s network, it is necessary to filter all incoming and outgoing network traffic. Because firewalls are typically the first line of defense against intruders, their configuration must be carefully implemented and tested before connections are established between internal networks and the Internet.

**Monitoring Tools**. Continuous monitoring of network activity is required if a site is to maintain confidence in the security of its network and data resources. Network monitors may be installed at strategic locations to collect and examine information continuously that may indicate suspicious activity. It is possible to have automatic notifications alert system administrators when the monitor detects anomalous readings, such as a burst of activity that may indicate a denial-of-service attempt. Such notifications may use a variety of channels, including electronic mail and mobile paging. Sophisticated systems capable of reacting to questionable network activity may be implemented to disconnect and block suspect connections, limit or disable affected services, isolate affected systems, and collect evidence for subsequent analysis.

**Cryptography**

One of the primary reasons that intruders can be successful is that most of the information they acquire from a system is in a form that they can read and comprehend. One solution to this problem is, through the use of cryptography, to prevent intruders from being able to use the information that they capture.

Encryption is the process of translating information from its original form (called plaintext) into an encoded, incomprehensible form (called ciphertext). Decryption refers to the process of taking ciphertext and translating it back into plaintext. Any type of data may be encrypted, including digitized images and sounds.

Cryptography secures information by protecting its confidentiality. Cryptography can also be used to protect information about the integrity and authenticity of data. For example, checksums are often used to verify the integrity of a block of information. Cryptographic checksums (also called message digests) help prevent undetected modification of information by encrypting the checksum in a way that makes the checksum unique.

The authenticity of data can be protected in a similar way. For example, to transmit information to a colleague by email, the sender first encrypts the information to protect its confidentiality and then attaches an encrypted digital signature to the message. When the colleague receives the message, he or she checks the origin of the message by using a key to verify the sender’s digital signature and decrypts the information using the corresponding decryption key.

**Notes:**

**MD5sum** –программа, позволяющая вычислять значения хеш-сумм (контрольных сумм) файлов по алгоритму MD5.

**Assignments**

**1. Translate the sentences from the texts into Russian in writing paying attention to the underlined words and phrases:**

1. In the face of the vulnerabilities and incident trends, a robust defenserequires a flexible strategy that allows adaptation to the changing environment, well-defined policies and procedures, the use of robust tools, and constant vigilance.
2. Factors that contribute to the success of a security policy include management commitment, technological support for enforcing the policy, effective dissemination of the policy, and the security awareness of all users.
3. Procedures address such topics as retrieving programs from the network, connecting to the site’s system from home or while traveling, using encryption, authentication for issuing accounts, configuration**,** and monitoring.
4. Intruders often install packet sniffers to capture passwords as theytraverse networks during remote login processes.
5. They squash the emissions of the genuine hostusing a denial-of-service attack and then attempt to connect to a target system using the address of the genuine host. To counter these address-spoofing attacksand enforce limitations on authorized connections into the organization’s network, it is necessary to filter all incoming and outgoing network traffic.
6. Sophisticated systems capable of reacting to questionable network activity may be implemented to disconnect and block suspect connections, limit or disable affected services, isolate affected systems, and collect evidence for subsequent analysis.
7. When the colleague receives the message, he or she checks the origin of the message by using a keyto verify the sender’s digital signature and decrypts the information using the corresponding decryption key.

**2. Answer the following questions:**

1. How can management contribute to the development of the security policy?
2. What are good security practices for the users?
3. What are the advantages of a one-time password?
4. How can the authenticity of data be protected?
5. What is a checksum for?

**3. Translate into English:**

**Меры по защите.**

1)Установите файрволл (firewall).2) Установите анти­вирусное и антишпионское ПО. Антивирусное ПО должно запускаться автоматически при загрузке Windows и рабо­тать постоянно, проверяя запускаемые вами программы в фоновом режиме. Обязательно проверяйте на вирусы пе­ред первым запуском любые программы, которые вы где-либо скачиваете или покупаете. 3) Не устанавливайте или удалите лишние ненужные службы Windows, которые не используете. Это ограничит возможности хакеров по дос­тупу к вашему компьютеру. 4) Не открывайте подозритель­ные письма странного происхождения, не поддавайтесь на содержащиеся в них сомнительные предложения лёгкого заработка, не высылайте никому пароли от ваших аккаун­тов, не открывайте прикреплённые к письмам подозри­тельные файлы и не переходите по содержащимся в них подозрительным ссылкам. 5) Не используйте простые па­роли. Не используйте один и тот же пароль на все случаи жизни. 6) Будьте осторожны при выходе в Интернет из мест общего пользования (например, Интернет-кафе), а также при использовании прокси-серверов. Пароли, который вы вводите, в этом случае, с большей вероятностью могут быть украдены. 7) При использовании электронных платёжных систем типа webmoney или Яндекс-деньги, работа с ними через веб-интерфейс является менее безопасной, чем если вы скачаете и установите специальную программу (webmoney keeper).

**4. Give the summary of the text using the key terms.**

**BIOMETRIC SECURITY TECHNOLOGY**

**Read the following words and word combinations and use them for understanding and translation of the text:**

**to forge** - подделать

**retina -** сетчатка

**iris** — радужка (глаза)

**gait** - походка

**moire fringe patterns** — интерференционный муар

**ultrasonics** — ультразвуковое излучение

**optical coupler** — оптический разветвитель

**pupil** - зрачок

**template-matching** — сравнение с шаблонами

**scam artist** - аферист

**frequent-flyer** — постоянный авиапассажир

**lock-down** — запор, блокировка

**sensitive data** — уязвимые данные

**to enlist** — включить в список

**covert surveillance** — скрытое наблюдение

**template** - шаблон

Biometrics is gaining increasing attention these days. Security systems, having realized the value of biometrics, use biometrics for two basic purposes: to verify or identify users. There are a number of biometrics and different applications need different biometrics.

Biometric is the most secure and convenient authentication tool. It can not be borrowed, stolen, or forgotten and forging one is practically impossible. Biometrics measure individual's unique physical or behavioral characteristics to recognize or authenticate their identity. Common physical biometrics include fingerprints, hand or palm geometry, retina, iris, and facial characteristics. Behavioral characters characteristics include signature, voice, keystroke pattern, and gait. Of this class of biometrics, technologies for signature and voice are the most developed.

There are many biometric technologies to suit different types of applications. Here comes a list of biometrics:

**Fingerprints** - A fingerprint looks at the patterns found on a fingertip. There are a variety of approaches to fingerprint verification, such as traditional police method, using pattern-matching devices, and things like moire fringe patterns and ultrasonics. This seems to be a very good choice for in-house systems.

**Hand geometry.** This involves analyzing and measuring the shape of the hand. It might be suitable where there are more users or where users access the system infrequently. Accuracy can be very high if desired, and flexible performance tuning and configuration can accommodate a wide range of applications. Organizations are using hand geometry readers in various scenarios, including time and attendance recording.

**Retina.** A retina-based biometric involves analyzing the layer of blood vessels situated at the back of the eye. This technique involves using a low intensity light source through an optical coupler to scan the unique patterns of the retina. Retinal scanning can be quite accurate but does require the user to look into a receptacle and focus on a given point.

**Iris.** An iris-based biometric involves analyzing features found in the colored ring of tissue that surrounds the pupil. This uses a fairly conventional camera element and requires no close contact between the user and the reader. Further, it has the potential for higher than average template-matching performance.

**Face.** Face recognition analyses facial characteristics. It requires a digital camera to develop a facial image of the user for authentication. Because facial scanning needs extra peripheral things that are not included in basic PCs, it is more of a niche market for network authentication. However, the casino industry has capitalized on this technology to create a facial database of scam artists for quick detection by security personnel.

**Signature.** Signature verification analyses the way user signs his name. Signing features such as speed, velocity, and pressure are as important as the finished signature's static shape. People are used to signatures as a means of transaction-related identity verification.

**Voice.** Voice authentication is based on voice-to-print authentication, where complex technology transforms voice into text. Voice biometrics requires a microphone, which is available with PCs nowadays. Voice biometrics is to replace the currently used methods, such as PINs, passwords, or account names. But voice will be a complementary technique for finger-scan technology as many people see finger scanning as a higher authentication form.

**Uses of Biometrics**

For decades, many highly secure environments have used biometric technology for entry access. Today, the primary application of biometrics is in physical security: to control access to secure locations (rooms or buildings). Biometrics permit unmanned access control. Biometric devices, typically hand geometry readers, are in office buildings, hospitals, casinos, health clubs and lodges. Biometrics are useful for high-volume access control. There are several promising prototype biometric applications. One of them, EyeTicket, links a passenger's frequent-flyer number to an iris scan. Some of the US airports use a sort of hand geometry biometric technology for performing citizen-verification functions.

It is also expected that virtual access is the application that will move biometrics for network and computer access. Physical lock-downs can protect hardware, and passwords are currently the most popular way to protect data on a network. Biometrics can increase a company's ability to protect its sensitive data by implementing a more secure key than a password. Using biometrics also allows a hierarchical structure of data protection, making the data even more secure. Biometric technologies further help to enhance security levels of access to network data.

E-commerce developers are exploring the use of biometrics and smart cards to more accurately verify a trading party's identity. Banks are bound to use this combination to better authenticate customers and ensure non-repudiation of online banking, trading and purchasing transactions. Point-of-sales (POS) system vendors are working on the cardholder verification method, which would enlist smart cards and biometrics to replace signature verification. Biometrics can help to obtain secure services over the telephone through voice authentication..

The last interesting application is for covert surveillance. Using facial and body recognition technologies, researchers hope to use biometrics to automatically identify known suspects entering buildings or traversing crowded security areas such as airports.

**Future Research Directions**

Although companies are using biometrics for authentication in a variety of situations, biometric technologies are evolving and emerging towards a large scale of use. Standards are coming out to provide a common software interface to allow sharing of biometric templates and to permit effective comparison and evaluation of different biometric technologies. One of them is the Common Biometric Exchange File Format, which defines a common means of exchanging and storing templates collected from a variety of biometric devices.

Biometric assurance - confidence that a biometric can achieve the intended level of security - is another active research area. Another interesting thing to be examined is combining biometrics with smart cards and public-key infrastructure (PKI). A major problem with biometrics is how and where to store the user's template. Because the template represents the user's personal characters, its storage introduces privacy concerns. Also storing the template in a centralized database paves for attack and compromise. On the other hand, storing the template on a smart card enhances individual privacy and increased protection from attack, because individual users control their own templates. Vendors enhance security by placing more biometric functions directly on the smart card. Some vendors like Biometric Associates, have built a fingerprint sensor directly into the smart card reader, which in turn passes the biometric to the smart card for verification.

PKI uses public- and private-key cryptography for user identification and authentication. It has some advantages over biometrics as it is mathematically more secure and it can be used across the Internet. The main drawback of PKI is the management of the user's private key. To be secure, the private key must be protected from compromise and to be useful, the private key must be portable. The solution is to store the private key on a smart card and protect it with biometric. There are proposals for integrating biometrics, smart cards and PKI technology for designing Smart Access common government ID cards.

**Notes:**

**PIN (Personal Identification Number)** – личный опознава­тельный номер, аналог пароля.

**EyeTicket** – программное обеспечение для распознавания пассажира по радужной оболочке глаза.

**Smart card** – пластиковая карта со встроенной микросхе­мой, контролирующей устройство и доступ к объектам па­мяти.

**Common Biometric Exchange File Format** – единый формат представления биометрических данных.

**Point-of-Sales system** – программно-аппаратный комплекс, функционирующий на базе фискального регистратора. За системой закреплен типичный набор кассовых функций.

**PKI (Public Key Infrustructure)** – инфраструктура открытых ключей. Набор средств, распределенных служб и компо­нентов, используемых для поддержки криптозадач на ос­нове открытого и закрытого ключей.

**ID (Identifier)** – идентификатор, уникальный признак объ­екта, позволяющий отличать его от других объектов.

**Assignments**

**1. Translate the sentences from the texts into Russian in writing paying attention to the underlined words and phrases:**

1. Common physical biometrics include fingerprints, hand or palm geometry, retina, iris, and facial characteristics. Behavioral characters characteristics include signature, voice, keystroke pattern, and gait.
2. There are a variety of approaches to fingerprint verification, such as traditional police method, using pattern-matching devices, and things like moire fringe patterns and ultrasonics. This seems to be a very good choice for in-house systems.
3. Accuracy can be very high if desired, and flexible performance tuning and configuration can accommodate a wide range of applications.
4. A retina-based biometric involves analyzing the layer of blood vessels situated at the back of the eye. This technique involves using a low intensity light source through an optical coupler to scan the unique patterns of the retina.
5. An iris-based biometric involves analyzing features found in the colored ring of tissue that surrounds the pupil.
6. Voice authentication is based on voice-to-print authentication, where complex technology transforms voice into text.
7. There are several promising prototype biometric applications. One of them, EyeTicket, links a passenger's frequent-flyer number to an iris scan.
8. Point-of-sales (POS) system vendors are working on the cardholder verification method, which would enlist smart cards and biometrics to replace signature verification.
9. Some vendors like Biometric Associates, have built a fingerprint sensor directly into the smart card reader, which in turn passes the biometric to the smart card for verification.

**2. Answer the following questions:**

1. What is the goal of biometrics?
2. Why is biometrics the most secure means of security?
3. What are biometric technologies? Characterize them in brief.
4. How can biometrics be used for secure network and computer access?
5. Why does storing a user's biometrics templates present a problem?

**3. Translate into English:**

На данный момент системы распознавания по отпечат­кам пальцев занимают более половины биометрического рынка. Множество российских и зарубежных компаний за­нимаются производством систем управления доступом, ос­нованных на методе дактилоскопической идентификации. По причине того, что это направление является одним из самых давнишних, оно получило наибольшее распростра­нение и является на сегодняшний день самым разработан­ным. Сканеры отпечатков пальцев прошли действительно длинный путь к улучшению. Современные системы осна­щены различными датчиками (температуры, силы нажатия и т.п.), которые повышают степень защиты от подделок. С каждым днем системы становятся все более удобными и компактными. По сути, разработчики достигли уже не­коего предела в данной области, и развивать метод дальше некуда. Кроме того, большинство компаний производят го­товые системы, которые оснащены всем необходимым, включая программное обеспечение. Интеграторам в этой области просто нет необходимости собирать систему само­стоятельно, так как это невыгодно и займет больше вре­мени и сил, чем купить готовую и уже недорогую при этом систему, тем более выбор будет действительно широк.

**4. Give the summary of the text using the key terms.**

**Topics for essays (you might need additional information):**

* An overview of possible threats and attacks.
* Technical trends affecting software security.
* Security goals.
* Preventive measures are the key point in the provision of software security.
* Identity theft.

**CRYPTOGRAPHY AND** **DATA ENCRYPTION**

**TERMINOLOGY**

**Read the following words and word combinations and use them for understanding and translation of the text:**

**thereof** - соответственно

**thorough** - тщательный

**undecipherable code** — код, не поддающийся расшифровке

**forgery** – подделка

**cipher** - шифр

**to derive from ...** – происходить из...

Cryptography and encryption have been used for secure communication for thousands of years.

Throughout history, military communication has had the greatest influence on encryption and the advancements thereof. The need for secure commercial and private communication has been led by the Information Age, which began in the 1980s. Although the Internet had been invented in the late 1960s, it did not gain a public face until the World Wide Web was invented in 1989. This new method of information exchange has caused a tremendous need for information security. A thorough understanding of cryptography and encryption will help people develop better ways to protect valuable information as technology becomes faster and more efficient.

**Cryptography** is the science or study of techniques of secret writing and message hiding. Cryptography constitutes any method in which someone attempts to hide a message, or the meaning thereof, in some medium.

**Encryption** is one specific element of cryptography in which one hides data or information by transforming it into an undecipherable code. Encryption typically uses a specified parameter or key to perform the data transformation. Some encryption algorithms require the key to be the same length as the message to be encoded, yet other encryption algorithms can operate on much smaller keys relative to the message. **Decryption** is often classified along with encryption as its opposite. Decryption of encrypted data results in the original data.

Encryption is used in everyday modern life. Encryption is most used among transactions over insecure channels of communication, such as the Internet. Encryption is also used to protect data being transferred between devices such as automatic teller machines (ATMs), mobile telephones, and many more. Encryption can be used to create digital signatures, which allow a message to be authenticated. When properly implemented, a digital signature gives the recipient of a message reason to believe the message was sent by the claimed sender. Digital signatures are very useful when sending sensitive email and other types of digital communication. This is relatively equivalent to traditional handwritten signatures, in that, a more complex signature carries a more complex method of forgery.

**A cipher** is an algorithm, process, or method for performing encryption and decryption. A cipher has a set of well-defined steps that can be followed to encrypt and decrypt messages. The operation of a cipher usually depends largely on the use of an encryption key. The key may be any auxiliary information added to the cipher to produce certain outputs.

**Plaintext and ciphertext** are typically opposites of each other. Plaintext is any information before it has been encrypted. Ciphertext is the output information of an encryption cipher. Many encryption systems carry many layers of encryption, in which the ciphertext output becomes the plaintext input to another encryption layer. The process of decryption takes ciphertext and transforms it back into the original plaintext.

In efforts to remain secure, governments have employed staff for studying encryption and the breaking thereof. **Cryptanalysis** is the procedures, processes, and methods used to translate or interpret secret writings or communication as codes and ciphers for which the key is unknown.

Even though the goal has been the same, the methods and techniques of cryptanalysis have changed drastically through time. These changes derive from an attempt to adapt to the increasing complexity of cryptography. Due to the tremendous advantage of knowing the enemy's thoughts, war is the main driving force of cryptanalysis. Throughout history many governments have employed divisions solely for cryptanalysis during war time. Within the last century, governments have employed permanent divisions for this purpose.

**Notes:**

**ATM (Automatic Teller Machine)** – банкомат

**Assignments**

**1. Translate the sentences from the text into Russian in writing paying attention to the underlined words and phrases:**

1. Throughout history, military communication has had the greatest influence on encryption and the advancements thereof.
2. Although the Internet had been invented in the late 1960s, it did not gain a public face until the World Wide Web was invented in 1989.
3. A thorough understanding of cryptography and encryption will help people develop better ways to protect valuable information as technology becomes faster and more efficient.
4. Cryptography constitutes any method in which someone attempts to hide a message, or the meaning thereof, in some medium.
5. When properly implemented, a digital signature gives the recipient of a message reason to believe the message was sent by the claimed sender. Digital signatures are very useful when sending sensitive email and other types of digital communication.
6. Plaintext is any information before it has been encrypted.
7. Ciphertext is the output information of an encryption cipher.
8. Due to the tremendous advantage of knowing the enemy's thoughts, war is the main driving force of cryptanalysis.
9. Throughout history many governments have employed divisions solely for cryptanalysis during war time.

**2. Answer the following questions:**

1. What is the difference between cryptography and cryptanalysis?
2. How can encryption be used in everyday life?
3. What does the operation of the cipher depend on?
4. What are the interrelations of a plaintext and ciphertext?
5. What is the main driving force of cryptanalysis?

**3. Translate into English:**

Криптография — наука о математических методах обеспечения конфиденциальности и аутентичности ин­формации. Изначально криптография изучала методы шифрования информации — обратимого преобразования открытого (исходного) текста на основе секретного алго­ритма и/или ключа в шифрованный текст (шифртекст). Традиционная криптография образует раздел симметрич­ных криптосистем, в которых зашифрование и расшифро­вание проводится с использованием одного и того же сек­ретного ключа. Помимо этого раздела современная крипто­графия включает в себя асимметричные криптосистемы, системы электронной цифровой подписи, хеш-функции, управление ключами, получение скрытой информации, квантовую криптографию.

Криптоанализ — наука о методах получения исходного значения зашифрованной информации, не имея доступа к секретной информации (ключу), необходимой для этого. В большинстве случаев под этим подразумевается нахожде­ние ключа. В нетехнических терминах, криптоанализ есть взлом шифра (кода).

Под термином «криптоанализ» также понимается по­пытка найти уязвимость в криптографическом алгоритме или протоколе. Результаты криптоанализа конкретного шифра называют криптографической атакой на этот шифр. Успешную криптографическую атаку, полностью дискредитирующую атакуемый шифр, называют взломом или вскрытием.

**4. Give the summary of the text using the key terms.**

**HISTORICAL CRYPTOGRAPHY**

**Read the following words and word combinations and use them for understanding and translation of the text:**

**scribe** - переписчик

**inscription** - надпись

**substitution cipher** - подстановочный шифр

**parchment** - пергамент

**to wind** - наматывать

**length-wise** - по длине

**a transposition cipher** - перестановочный шифр

**to overtake** - опережать

**grid** - решетка

**offset** - сдвинутый

**gibberish** - бессмысленный

**to intercept** - перехватывать

**brute force method** - подбор методом грубой силы

**overconfidence** - самонадеянность

**to map** - преобразовать

**stepping switch** - шаговый переключатель

**renowned** - прославленный

**Ancient Egypt**

The earliest known text containing components of cryptography originates in the Egyptian town Menet Khufu on the tomb of nobleman Khnumhotep II nearly 4,000 years ago. In about 1900 B.C. Khnumhotep's scribe drew his master's life in his tomb. As he drew the hieroglyphics he used a number of unusual symbols to obscure the meaning of the inscriptions. This method of encryption is an example of a substitution cipher, which is any cipher system which substitutes one symbol or character for another.

As the Egyptian culture evolved, hieroglyphic substitution became more common. This method of encryption was relatively easy to break for those who could read and write. There are several possibilities why the Egyptians would use the sacred nature of their religious rituals from common cryptography is that the scribes wanted to give a formal appearance to their writings. This seems to be very similar to formal complicated language used in any modern legal document. Egyptian cryptography could also have been a way for a scribe to impress others by showing that he could write at a higher level.

**Greece**

In about 500 B.C. the Spartans developed a device called Scytale, which was used to send and receive secret messages. The device was a cylinder in which a narrow strip of parchment was wound. The message was then written length-wise on the parchment. Once it was unwound the message on the strip of parchment became unreadable. To receive the message an identical cylinder was needed. It was only then that the letters would line up resulting in the original message.

The Scytale is an example of a transposition cipher, which is any cipher system that changes the order of the characters rather than changing the characters themselves. In today's standards, the Scytale would be very easy to decipher, however, 2,500 years ago the percent of people that could read and write was relatively small. The Scytale provided the Spartans a secure method of communication.

**Rome**

The earliest recorded military use of cryptography comes from Julius Caesar 2,000 years ago. Caesar, being commander of the Roman army, solved the problem of secure communication with his troops. The problem was that messengers of secret military messages were often overtaken by the enemy. Caesar developed a substitution cipher method in which he would substitute letters for different letters. Only those who knew the substitution used could decipher the secret messages. Now when the messengers were overtaken the secret messages were not exposed. This gave the Roman army a huge advantage during war.

Caesar typically just shifted his letters by some predetermined number. This number was the cipher key of his algorithm. A randomized order of substitution yields a much larger amount of security due to the larger amount of possible orderings.

**Alberti-Vigenere Cipher**

During the mid 1400s a man named Leon Battista Alberti invented an encryption system using a cipher disk. This was a mechanical device with sliding disks that allowed for many different methods of substitution. This is the base concept of a polyalphabetic cipher, which is an encryption method which switches through several substitution ciphers throughout encryption. Alberti never developed his cipher disk concept.

In the 1500s Blaise De Vigenere, following Alberti's polyalphabetic cipher style, created a cipher that came to be known as the Vigenere Cipher. The Vigenere Cipher works exactly like the Caesar except that it changes the key throughout the encryption process. The Vigenere Cipher uses a grid of letters that give the method of substitution. This grid is called a Vigenere Square or a Vigenere Table. The grid is made up of 26 alphabets offset from each other by one letter.

The method of changing from one key to another follows one simple pattern. The encryption key was chosen as a special secret word. The corresponding letter is then substituted for the plaintext character. This method is repeated through all characters of the key word. After all characters of the key word are used, the word is just repeated.

**Jefferson Wheel Cipher**

In the late 1700s, Thomas Jefferson came up with a cipher system very similar to the Vigenere Cipher except with higher security. His invention was 26 wheels with the alphabet randomly scattered on each wheel. The wheels were numbered and ordered with a specified order. This order is the key to the encryption algorithm.

To message to be encrypted on the wheels lining up is made on the wheels such that the message is present. The ciphertext is any other line besides the line containing the original message. The person decrypting the ciphertext must have the wheels in the proper order. As the ciphertext is made on the wheels, the plaintext is lined up somewhere else on the wheels. A visual scan can quickly result in finding the original text. There is an extremely small chance that two non-gibberish messages will emerge on the disk during decryption.

**Zimmerman Telegram**

In early 1917, during the early stages of World War I, British cryptographers encountered a German encoded telegram. This telegram is often referred to as the Zimmerman Telegram. These cryptographers were able to decipher the telegram, and in doing so they changed cryptanalysis history. Using this deciphered message, they were able to convince the United States to join the war.

The Zimmerman Telegram was a secret communication between the Foreign Secretary of the German Empire, Arthur Zimmerman, and the German ambassador in Mexico, Heinrich von Eckardt. The telegram contained an offer for Mexico to reclaim its territory of New Mexico, Texas, and Arizona if it joined the German cause.

**Choctaw Codetalkers**

As WWI went on, the United States had the continuing problem of the lack of secure communication. Almost every phone call made was intercepted by the Germans, leaving every move made by the allies known to the Germans. Army commander, Captain Lewis devised a plan that utilized American Indian languages. He found eight Choctaw men in the battalion and used them to talk to each other over radio and phone lines. Their language was valuable because ordinary codes and ciphers of a shared language can be broken, whereas codes based on a unique language must be studied extensively before beginning to decode them. Within 24 hours of using the Choctaw language as encryption, the advantage fell in favor of the United States. Within 72 hours, the Germans were retreating and the allies were in full attack.

**Enigma Encryption Machine**

At the end of World War I, Arthur Scherbius invented the Enigma, an electro-mechanical machine that was used for encryption and decryption of secret messages. Because of the numerous configurations, the Enigma was virtually unbreakable with brute force methods.

It wasn't until World War II that the Enigma gained its fame. Due to the Enigma's statistical security, Nazi Germany became overconfident about their ability to encrypt secret messages. This overconfidence caused the downfall of the Enigma. Along with numerous German operator errors, the Enigma had several built-in weaknesses that Allied cryptographers exploited. The major weakness was that its substitution algorithm did not allow any letter to be mapped to itself. This allowed the Allied cryptographers to decrypt a vast number of ciphered messages sent by Nazi Germans.

**Purple**

While the Allied forces were focusing on cracking the German Enigma, the Japanese developed an encryption machine called Purple. In contrast to the Enigma's rotors, Purple was made using stepping switches commonly used for routing telephone signals. During the war, the Japanese were most efficient in destroying their encryption machines. Currently, not one complete Purple machine has been discovered.

Because the Japanese were so good at keeping their encryption methods secret, the United States cryptographers had a hard time decrypting their messages. William Friedman, a renowned cryptographer, and his team built a replica of Purple based only on the encrypted messages recovered. Because they had never seen a Purple machine and didn't know how it worked, this proved to be very difficult. Eventually the team figured out the encryption method used by Purple, and were able to build a different machine for the decryption of it. This advancement allowed the United States to access the Japanese diplomatic secrets in World War II.

**Notes:**

**Khnumhotep** – древнеегипетский высокопоставленный придворный вельможа.

**B.C. (Before Christ)** – до нашей эры.

**Scytale** – шифр Древней Спарты, прибор для перестано­вочного шифрования.

**Choctaw** – коренной народ США, проживавший изна­чально на юго-востоке.

**Assignments**

**1. Translate the sentences from the texts into Russian in writing paying attention to the underlined words and phrases:**

1. In about 1900 B.C. Khnumhotep's scribe drew his master's life in his tomb. As he drew the hieroglyphics he used a number of unusual symbols to obscure the meaning of the inscriptions.
2. The device was a cylinder in which a narrow strip of parchment was wound. The message was then written length-wise on the parchment.
3. The Scytale is an example of a transposition cipher, which is any cipher system that changes the order of the characters rather than changing the characters themselves
4. Only those who knew the substitution used could decipher the secret messages. Now when the messengers were overtaken the secret messages were not exposed.
5. A randomized order of substitution yields a much larger amount of security due to the larger amount of possible orderings.
6. There is an extremely small chance that two non-gibberish messages will emerge on the disk during decryption.
7. Because of the numerous configurations, the Enigma was virtually unbreakable with brute force methods.
8. The major weakness was that its substitution algorithm did not allow any letter to be mapped to itself.

**2. Answer the following questions:**

1. How does the substitution cipher work?
2. What is a Scytale?
3. What is a transposition cipher?
4. What idea underlies the Vegenere Cipher?
5. Why is it more difficult to break the code based on a unique language?
6. What is the Enigma known for?

**3. Translate into English:**

Криптография – тайнопись. Термин ввел Д. Валлис. Потребность шифровать и передавать шифрованные со­общения возникла очень давно. Так, еще в V-IV вв. до н. э. греки применяли специальное шифрующее устройство. По описанию Плутарха, оно состояло из двух палок одинако­вой длины и толщины. Одну оставляли себе, а другую от­давали отъезжающему. Эти палки называли скиталами. Ко­гда правителям нужно было сообщить какую-нибудь важ­ную тайну, тогда вырезали длинную и узкую, вроде ремня, полосу папируса, наматывали ее на свою скиталу, не остав­ляя на ней никакого промежутка, так чтобы вся поверх­ность палки была охвачена этой полосой. Затем, оставляя папирус на скитале в том виде, как он есть, писали на нем все, что нужно, а написав, снимали полосу и без палки от­правляли адресату. Так как буквы на ней разбросаны в бес­порядке, то прочитать написанное он мог, только взяв свою скиталу и намотав на нее без пропусков эту полосу.

Аристотелю принадлежит способ дешифрования этого шифра. Надо изготовить длинный конус и, начиная с осно­вания, обертывать его лентой с шифрованным сообще­нием, постепенно сдвигая ее к вершине. В какой-то момент начнут просматриваться куски сообщения. Так можно оп­ределить диаметр скиталы.

**4. Give the summary of the text using the key terms.**

**MODERN ENCRYPTION**

**Read the following words and word combinations and use them for understanding and translation of the text:**

**one-time pad** – блокнот одноразового использования

**to withstand** - противостоять

**prior to...** - перед чем-либо

**to be referred to as...** - называться

**flaw** - ошибка

**staggering** - ошеломляющий

**power (зд.)** - степень

**conventional computers** — традиционные компьютеры

**to listen in** - подслушать

**key distribution problem** — задача распределения ключей

Until the 1990s, cryptology was based on **algorithms** -- a mathematical process or procedure. These algorithms are used in conjunction with a **key**, a collection of bits (usually numbers). Without the proper key, it's virtually impossible to decipher an encoded message, even if you know what algorithm to use.

The **"one-time pad"** encryption algorithm was invented in the early 1900s, and has since been proven as unbreakable. The one-time pad algorithm is derived from a previous cipher called Vernam Cipher, named after Gilbert Vernam. The Vernam Cipher was a cipher that combined a message with a key read from a paper tape or pad. The Vernam Cipher was not unbreakable until Joseph Mauborgne recognized that if the key was completely random the cryptanalytic difficultly would be equal to attempting every possible key. Even when trying every possible key, one would still have to review each attempt at decipherment to see if the proper key was used. The unbreakable aspect of the one-time pad comes from two assumptions: the key used is completely random; and the key cannot be used more than once. The security of the one-time pad relies on keeping the key 100% secret. The one-time pad is typically implemented by using a modular addition (XOR) to combine plaintext elements with key elements. The key used for encryption is also used for decryption. Applying the same key to the ciphertext results back to the plaintext.

If any non-randomness occurs in the key of a one-time pad, the security is decreased and thus no more unbreakable. Numerous attempts have been made to create seemingly random numbers from a designated key. These number generators are called **Pseudo-Random Number Generators (PRNGs)** because they cannot give a completely random number stream. Even though the security of a PRNG is not 100% unbreakable, it can provide sufficient security when implemented correctly. PRNGs that have been designated secure for cryptographic use are called Cryptographically Secure Pseudo-Random Number Generators (CSPRNGs). CSPRNGs have qualities that other PRNGs do not. CSPRNGs must pass the "next-bit test" in that given the first k bits, there is no polynomial-time algorithm that can predict the (k+1)th bit with probability of success higher than 50%. CSPRNGs must also withstand "state compromises." In the event that part or all of its state is revealed, it should be impossible to reconstruct the stream of random numbers prior to the revelation.

There are limitless possibilities for keys used in cryptology. But there are only two widely used methods of employing keys: public-key cryptology and secret-key cryptology. In both of these methods (and in all cryptology), the sender (point A) is referred to as Alice. Point B is known as Bob.

In the **public-key cryptology** **(PKC)** method, a user chooses two interrelated keys. He lets anyone who wants to send him a message know how to encode it using one key. He makes this key public. The other key he keeps to himself. In this manner, anyone can send the user an encoded message, but only the recipient of the encoded message knows how to decode it. Even the person sending the message doesn't know what code the user employs to decode it.

PKC is often compared to a mailbox that uses two keys. One unlocks the front of the mailbox, allowing anyone with a key to deposit mail. But only the recipient holds the key that unlocks the back of the mailbox, allowing only him to retrieve the messages.

The other usual method of traditional cryptology is **secret-key cryptology** **(SKC)**. In this method, only one key is used by both Bob and Alice. The same key is used to both encode and decode the plaintext. Even the algorithm used in the encoding and decoding process can be announced over an unsecured channel. The code will remain uncracked as long as the key used remains secret.

SKC is similar to feeding a message into a special mailbox that grinds it together with the key. Anyone can reach inside and grab the cipher, but without the key, he won't be able to decipher it. The same key used to encode the message is also the only one that can decode it, separating the key from the message.

Both the secret-key and public-key methods of cryptology have unique flaws. The problem with public-key cryptology is that it's based on the staggering size of the numbers created by the combination of the key and the algorithm used to encode the message. These numbers can reach unbelievable proportions. What's more, they can be made so that in order to understand each bit of output data, you have to also understand every other bit as well. This means that to crack a 128-bit key, the possible numbers used can reach upward to the 1038 power. That's a lot of possible numbers for the correct combination to the key.

The keys used in modern cryptography are so large, in fact, that a billion computers working in conjunction with each processing a billion calculations per second would still take a trillion years to definitively crack a key. This isn't a problem now, but it soon will be. Current computers will be replaced in the near future with quantum computers, which exploit the properties of physics on the immensely small quantum scale. Since they can operate on the quantum level, these computers are expected to be able to perform calculations and operate at speeds no computer in use now could possibly achieve. So the codes that would take a trillion years to break with conventional computers could possibly be cracked in much less time with quantum computers. This means that secret-key cryptology (SKC) looks to be the preferred method of transferring ciphers in the future.

But SKC has its problems as well. The chief problem with SKC is how the two users agree on what secret key to use. It's possible to send a message concerning which key a user would like to use, but shouldn't that message be encoded, too? And how do the users agree on what secret key to use to encode the message about what secret key to use for the original message? There's almost always a place for an unwanted third party to listen in and gain information the users don't want that person to have. This is known in cryptology as the **key** distribution problem.

**RSA encryption**, named for the surnames of the inventors, relies on multiplication and exponentiation being much faster than prime factorization. The entire protocol is built from two large prime numbers. These prime numbers are manipulated to give a public key and private key. Once these keys are generated they can be used many times. Typically one keeps the private key and publishes the public key. Anyone can then encrypt a message using the public key and send it to the creator of the keys. This person then uses the private key to decrypt the message. Only the one possessing the private key can decrypt the message. One of the special numbers generated and used in RSA encryption is the modulus, which is the product of the two large primes. In order to break this system, one must compute the prime factorization of the modulus, which results in the two primes. The strength of RSA encryption depends on the difficultly to produce this prime factorization. RSA Encryption is the most widely used **asymmetric key encryption** system used for electronic commerce protocols.

**Notes:**

**One-time pad** (другое название **Vernam Cipher**) – система симметричного шифрования. Является единственной сис­темой шифрования, для которой доказана абсолютная криптографическая стойкость.

**XOR (Exclusive or)** – сложение по модулю 2, логическая и битовая операция.

**Pseudo-Random Number Generator** – генератор псевдослу­чайных чисел.

**Cryptographically Secure Pseudo-Random Number Generator** – криптографически безопасный генератор псев­дослучайных чисел.

**RSA encryption** (аббревиатура от имен Rivest, Shamir, and Adleman) – криптографический алгоритм с открытым клю­чом, основывающийся на вычислительной сложности за­дачи факторизации больших целых чисел.

**Assignments**

**1. Translate the sentences from the texts into Russian in writing paying attention to the underlined words and phrases:**

1. The "one-time pad" encryption algorithm was invented in the early 1900s, and has since been proven as unbreakable.
2. Even when trying every possible key, one would still have to review each attempt at decipherment to see if the proper key was used.
3. The one-time pad is typically implemented by using a modular addition (XOR) to combine plaintext elements with key elements.
4. Numerous attempts have been made to create seemingly random numbers from a designated key.
5. CSPRNGs must pass the "next-bit test" in that given the first k bits, there is no polynomial-time algorithm that can predict the (k+1)th bit with probability of success higher than 50%.
6. SKC is similar to feeding a message into a special mailbox that grinds it together with the key.
7. RSA encryption, named for the surnames of the inventors, relies on multiplication and exponentiation being much faster than prime factorization.
8. One of the special numbers generated and used in RSA encryption is the modulus, which is the product of the two large primes. In order to break this system, one must compute the prime factorization of the modulus, which results in the two primes.

**2. Answer the following questions:**

1. Is the one-time pad an unbreakable means of encryption?
2. What two assumptions does the unbreakable aspect of the one-time pad come from?
3. What is the difference between PRNG and CSPRNG?
4. What is safer: PKC or SKC?
5. What can the strength of RSA encryption depend on?

**3. Translate into English:**

Как бы ни были сложны и надежны криптографиче­ские системы, их слабое место при практической реализа­ции - проблема распределения ключей. Для того, чтобы был возможен обмен конфиденциальной информацией между двумя субъектами ИС, ключ должен быть сгенери­рован одним из них, а затем каким-то образом опять же в конфиденциальном порядке передан другому. Т.е. в общем случае для передачи ключа опять же требуется использова­ние какой-то криптосистемы.

Для решения этой проблемы на основе результатов, полученных классической и современной алгеброй, были предложены системы с открытым ключом.

Суть их состоит в том, что каждым адресатом ИС гене­рируются два ключа, связанные между собой по опреде­ленному правилу. Один ключ объявляется открытым, а другой закрытым. Открытый ключ публикуется и доступен любому, кто желает послать сообщение адресату. Секрет­ный ключ сохраняется в тайне.

Исходный текст шифруется открытым ключом адре­сата и передается ему. Зашифрованный текст в принципе не может быть расшифрован тем же открытым

**4. Give the summary of the text using the key terms.**

**FUTURE METHODS OF ENCRYPTION**

**Read the following words and word combinations and use them for understanding and translation of the text:**

**eavesdropper** - перехватчик

**to harness** — приспособить, поставить на службу

**spin** - вращение

**binary code** – двоичный код

**coherent** - понятный

**to accomplish** - выполнять

**to discard** - отбрасывать

**discrepancy** - несоответствие

**parity check** — контроль четности

**to bounce** - отскакивать

**spooky** — жуткий, зловещий

**entanglement** - переплетение

**fiber optic cable** – оптоволоконный кабель

**Quantum Cryptology**

One of the great challenges of cryptology is to keep unwanted parties – or **eavesdroppers** - from learning of sensitive information. Quantum physics has provided a way around this problem. By harnessing the unpredictable nature of matter at the quantum level, physicists have figured out a way to exchange information on secret keys.

Quantum cryptography uses photons to transmit a key. Once the key is transmitted, coding and encoding using the normal secret-key method can take place. But how does a photon become a key? How do you attach information to a photon's spin?

This is where **binary code** comes into play. Each type of a photon's spin represents one piece of information - usually a 1 or a 0, for binary code. This code uses strings of 1s and 0s to create a coherent message. So a binary code can be assigned to each photon. Alice can send her photons through randomly chosen filters and record the polarization of each photon. She will then know what photon polarizations Bob should receive. Bob has no idea what filter to use for each photon, he's guessing for each one. After the entire transmission, Bob and Alice have a non-encrypted discussion about the transmission.

The reason this conversation can be public is because of the way it's carried out. Bob calls Alice and tells her which filter he used for each photon, and she tells him whether it was the correct or incorrect filter to use. Since Bob isn't saying what his measurements are - only the type of filter he used - a third party listening in on their conversation can't determine what the actual photon sequence is.

In modern cryptology, Eve (E – an eavesdropper) can **passively intercept** Alice and Bob's encrypted message - she can get her hands on the encrypted message and work to decode it without Bob and Alice knowing she has their message. Eve can accomplish this in different ways, such as wiretapping Bob or Alice's phone or reading their secure e-mails.

Quantum cryptology is the first cryptology that safeguards against passive interception. Here's an example. If Alice sends Bob a series of polarized photons, and Eve has set up a filter of her own to intercept the photons, Eve is in the same boat as Bob: Neither has any idea what the polarizations of the photons Alice sent are. Like Bob, Eve can only guess which filter orientation she should use to measure the photons.

After Eve has measured the photons by randomly selecting filters to determine their spin, she will pass them down the line to Bob. She does to cover up her presence and the fact that she intercepted the photon message. But Eve's presence will be detected. By measuring the photons, Eve inevitably altered some of them.

Alice and Bob can further protect their transmission by discussing some of the exact correct results after they've discarded the incorrect measurements. This is called a **parity check**. If the chosen examples of Bob's measurements are all correct - meaning the pairs of Alice's transmitted photons and Bob's received photons all match up - then their message is secure.

Bob and Alice can then discard these discussed measurements and use the remaining secret measurements as their key. If discrepancies are found, they should occur in 50 percent of the parity checks. Since Eve will have altered about 25 percent of the photons through her measurements, Bob and Alice can reduce the likelihood that Eve has the remaining correct information down to a one-in-a-million chance by conducting 20 parity checks.

**Quantum Cryptology Problems**

Despite all of the security it offers, quantum cryptology also has a few fundamental flaws. Chief among these flaws is the length under which the system will work: It’s too short.

The original quantum cryptography system, built in 1989 by Charles Bennett, Gilles Brassard and John Smolin, sent a key over a distance of 36 centimeters. Since then, newer models have reached a distance of 150 kilometers (about 93 miles). But this is still far short of the distance requirements needed to transmit information with modern computer and telecommunication systems.

The reason why the length of quantum cryptology capability is so short is because of interference. A photon’s spin can be changed when it bounces off other particles, and so when it's received, it may no longer be polarized the way it was originally intended to be. As the distance a photon must travel to carry its binary message is increased, so, too, is the chance that it will meet other particles and be influenced by them.

One group of Austrian researchers may have solved this problem. This team used what Albert Einstein called “spooky action at a distance.” This observation of quantum physics is based on the **entanglement** of photons. At the quantum level, photons can come to depend on one another after undergoing some particle reactions, and their states become entangled. This entanglement doesn’t mean that the two photons are physically connected, but they become connected in a way that physicists still don't understand. In entangled pairs, each photon has the opposite spin of the other. If the spin of one is measured, the spin of the other can be deduced. What’s strange (or “spooky”) about the entangled pairs is that they remain entangled, even when they’re separated at a distance.

The Austrian team put a photon from an entangled pair at each end of a fiber optic cable. When one photon was measured in one polarization, its entangled counterpart took the opposite polarization, meaning the polarization the other photon would take could be predicted. It transmitted its information to its entangled partner. This could solve the distance problem of quantum cryptography, since there is now a method to help predict the actions of entangled photons.

Even though it’s existed just a few years so far, quantum cryptography may have already been cracked. A group of researchers from Massachusetts Institute of Technology took advantage of another property of entanglement. In this form, two states of a single photon become related, rather than the properties of two separate photons. By entangling the photons the team intercepted, they were able to measure one property of the photon and make an educated guess of what the measurement of another property - like its spin - would be. By not measuring the photon’s spin, they were able to identify its direction without affecting it. So the photon traveled down the line to its intended recipient none the wiser.

The MIT researchers admit that their eavesdropping method may not hold up to other systems, but that with a little more research, it could be perfected. Hopefully, quantum cryptology will be able to stay one step ahead as decoding methods continue to advance.

**Assignments**

**1. Translate the sentences from the texts into Russian in writing paying attention to the underlined words and phrases:**

1. By harnessing the unpredictable nature of matter at the quantum level, physicists have figured out a way to exchange information on secret keys.
2. After the entire transmission, Bob and Alice have a non-encrypted discussion about the transmission.
3. Since Bob isn't saying what his measurements are -- only the type of filter he used -- a third party listening in on their conversation can't determine what the actual photon sequence is.
4. One of the great challenges of cryptology is to keep unwanted parties – or eavesdroppers -- from learning of sensitive information.
5. In modern cryptology, Eve (E – an eavesdropper) can passively intercept Alice and Bob's encrypted message -- she can get her hands on the encrypted message and work to decode it without Bob and Alice knowing she has their message.
6. After Eve has measured the photons by randomly selecting filters to determine their spin, she will pass them down the line to Bob.
7. If discrepancies are found, they should occur in 50 percent of the parity checks. Since Eve will have altered about 25 percent of the photons through her measurements, Bob and Alice can reduce the likelihood that Eve has the remaining correct information down to a one-in-a-million chance by conducting 20 parity checks.
8. As the distance a photon must travel to carry its binary message is increased, so, too, is the chance that it will meet other particles and be influenced by them.
9. At the quantum level, photons can come to depend on one another after undergoing some particle reactions, and their states become entangled.

**2. Answer the following questions:**

1. How can quantum physics help users to exchange information securely?
2. How does a photon become a key?
3. Can the users communicate openly using photons for encryption?
4. How can quantum cryptology safeguard against passive interception?
5. How does the parity check work?
6. What are the main flaws of quantum cryptology?
7. Is it possible to increase the quantum cryptology capability?

**3. Translate into English:**

Наибольшее практическое применение КК находит се­годня в сфере защиты информации, передаваемой по *воло­конно-оптическим линиям связи (ВОЛС*). Это объясняется тем, что оптические волокна ВОЛС позволяют обеспечить пере­дачу фотонов на большие расстояния с минимальными ис­кажениями. В качестве источников фотонов применяются лазерные диоды передающих модулей ВОЛС; далее проис­ходит существенное ослабление мощности светового сиг­нала - до уровня, когда среднее число фотонов на один им­пульс становится много меньше единицы. Системы пере­дачи информации по ВОЛС, в приемном модуле которых применяются лавинные фотодиоды в режиме счета фото­нов, называются *квантовыми оптическими каналами связи (КОКС).*

Понятно, что вследствие малой энергетики сигналов скорости передачи информации в КОКС по сравнению с возможностями современных ВОЛС не слишком высоки (от килобит до мегабит в секунду, в зависимости от реализа­ции). Поэтому в большинстве случаев *квантовые крипто­графические системы (ККС)*применяются для распределе­ния ключей, которые затем используются средствами шифрования высокоскоростного потока данных. Необхо­димо отметить, что квантово-криптографическое оборудо­вание пока серийно не выпускается. Однако по мере со­вершенствования и удешевления применяемой элементной базы можно ожидать появления ККС на рынке телекомму­никаций в качестве, например, дополнительной услуги при построении корпоративных волоконно-оптических сетей.

**4. Give the summary of the text using the key terms.**

**Topics for essays (you might need additional information):**

* The Information Age and the increased vulnerability of sensitive data.
* Cryptography, cryptology, cryptanalysis, and their interrelation.
* Historical insight into the development of cryptography and cryptology.
* The evolution of modern encryption.
* The challenges of quantum cryptology.

**COMPUTER GRAPHICS**

**HISTORY AND DEVELOPMENT**

**Read the following words and word combinations and use them for understanding and translation of the text:**

**in a sense** - в широком смысле

**to be widespread** - быть распространенным

**to improve** - улучшать

**to emerge** - возникать, появляться

**visual content** - визуальное содержание

**rendering** - передача

**to be coined by** - быть созданным

**amendable** - поддающийся улучшению

**to be hooked up to** - быть подключенным к чему-либо

**forbidding** - запрещающий

**non-obvious uses** - неявные, неосновные использования

The term computer graphics has been used in a broad sense to describe "almost everything on computers that is not text or sound".

Computer graphics is widespread today. The computer imagery is found on television, in newspapers, for example in weather reports, or for example in all kinds of medical investigation and surgical procedures. A well-constructed graph can present complex statistics in a form that is easier to understand and interpret. In the media "such graphs are used to illustrate papers, reports, thesis", and other presentation material.

Many powerful tools have been developed to visualize data. Computer generated imagery can be categorized into several different types: 2D, 3D, and animated graphics. As technology has improved, 3D computer graphics have become more common, but 2D computer graphics are still widely used. Computer graphics has emerged as a sub-field of computer science which studies methods for digitally synthesizing and manipulating visual content. Over the past decade, other specialized fields have been developed like information visualization, and scientific visualization more concerned with "the visualization of three dimensional phenomena (architectural, meteorological, medical, biological, etc.), where the emphasis is on realistic renderings of volumes, surfaces, illumination sources, and so forth, perhaps with a dynamic (time) component".

The phrase “Computer Graphics” was coined in 1960 by William Fetter, a graphic designer for Boeing. The field of computer graphics developed with the emergence of computer graphics hardware. Early projects like the Whirlwind and SAGE Projects introduced the CRT as a viable display and interaction interface and introduced the light pen as an input device.

Most early mainframe business computers produced out- put only in the form of punched cards, paper tape, or text printouts. However, system designers realized that some kinds of data were particularly amenable to a graphical representation. In the early 1950s, the first systems using the cathode ray tube (CRT) for graphics output found specialized application. For example, the MIT Whirlwind and the Air Force’s SAGE air defense system used a CRT to display information such as the location and heading of radar targets. By the late 1970s, the microcomputers from Apple, Radio Shack, Commodore, and others either included CRT monitors or had adapters that allowed them to be hooked up to regular television sets. These machines generally came with a version of the BASIC language that included commands for plotting lines and points and filling enclosed figures with color. While crude by modern standards, these graphics capabilities meant that spreadsheet programs could provide charts while games and simulations could show moving, interacting objects. Desktop computers showed pictures on television-like screens. Research at the Xerox PARC laboratory in the 1970s demonstrated the advantages of a graphical user interface based on visual objects, including menus, windows, dialog boxes, and icons.

The Apple Macintosh, introduced in 1984, was the first commercially viable computer in which everything displayed on the screen (including text) consisted of bitmapped graphics. Microsoft’s similar Windows operating environment became dominant on IBM architecture PCs during the 1990s.

Today Apple, Microsoft, and UNIX-based operating systems include extensive graphics functions. Game and multimedia developers can call upon such facilities as Apple QuickDraw and Microsoft Directx to create high resolution, realistic graphics.

**What is computer graphics used for?**

Obvious uses of computer graphics include computer art, CGI films, architectural drawings, and graphic design — but there are many non-obvious uses as well and not all of them are "artistic." Scientific visualization is a way of producing graphic output from computer models so it's easier for people to understand. Computerized models of global warming produce vast tables of numbers as their output, which only a PhD in climate science could figure out; but if you produce a speeded-up animated visualization — with the Earth getting bluer as it gets colder and redder as it gets hotter — anyone can understand what's going on. Medical imaging is another good example of how graphics make computer data more meaningful. When doctors show you a brain or body scan, you're looking at a computer graphic representation drawn using vast amounts of data produced from thousands or perhaps even millions of measurements. The jaw-dropping photos beamed back from space by amazing devices like the Hubble Space Telescope are usually enhanced with the help of a type of computer graphics called image processing; that might sound complex, but it's not so very different from using a graphics package like Google Picasa or PhotoShop to touch up your holiday snaps).

And that's really the key point about computer graphics: they turn complex computer science into everyday art we can all grasp, instantly and intuitively. Back in the 1980s, when programming a Commodore PET, the only way to get it to do anything was to type meaningless little words like PEEK and POKE onto a horribly unfriendly green and black screen. Virtually every modern computer now has what's called a GUI (graphical user interface), which means you operate the machine by pointing at things you want, clicking on them with your mouse or your finger, or dragging them around your "desktop." It makes so much more sense because we're visual creatures: something like a third of our cortex (higher brain) is given over to processing information that enters our heads through our eyes. That's why a picture really is worth a thousand words (sometimes many more) and why computers that help us visualize things with computer graphics have truly revolutionized the way we see the world.

**Notes:**

**CRT** - мониторы (Cathode Ray Tube) - самый распростра­ненный тип. Как видно из названия, в основе всех подоб­ных мониторов лежит катодно-лучевая трубка, или, как принято говорить в отечественной литературе, электронно-лучевая трубка (ЭЛТ).

**Microsoft Directx** - Microsoft DirectX - это ряд технологий, благодаря которым компьютеры на основе Windows стано­вятся идеальной средой для запуска и отображения прило­жений, богатых элементами мультимедиа, такими как цветная графика, видео, трехмерная анимация и стерео­звук. DirectX включает обновления, повышающие безопас­ность и производительность, а также новые функции, отно­сящиеся к различным технологиям, к которым приложение может обращаться с помощью DirectX API.

**Assignments**

**1. Translate the sentences from the texts into Russian in writing paying attention to the underlined words and phrases:**

1. A well-constructed graph can present complex statistics in a form that is easier to understand and interpret.
2. Many powerful tools have been developed to visualize data.
3. Over the past decade, other specialized fields have been developed like information visualization.
4. The phrase “Computer Graphics” was coined in 1960 by William Fetter.
5. The field of computer graphics developed with the emergence of computer graphics hardware.
6. By the late 1970s, the microcomputers from Apple, Radio Shack, Commodore, and others either included CRT monitors or had adapters that allowed them to be hooked up to regular television sets.

**2. Answer the following questions:**

1. Where can the computer imagery be seen?
2. From what sub-field of computer science did the computer graphics emerge?
3. Who coined the term “computer graphics”?
4. What are the main steps of computer graphics development?
5. What are the main fields of computer graphiсs application?

**3. Translate into English:**

Область применения компьютерной графики не огра­ничивается одними художественными эффектами. Во всех отраслях науки, техники, медицины, в коммерческой и управленческой деятельности используются построенные с помощью компьютера схемы, графики, диаграммы, пред­назначенные для наглядного отображения разнообразной информации. Конструкторы, разрабатывая новые модели автомобилей и самолетов, используют трехмерные графи­ческие объекты, чтобы представить окончательный вид из­делия. Архитекторы создают на экране монитора объемное изображение здания, и это позволяет им увидеть, как оно впишется в ландшафт.

**4. Give the summary of the text using the key terms.**

**CONCEPTS AND PRINCIPLES**

**Read the following words and word combinations and use them for understanding and translation of the text:**

**binary format** - двоичный формат

**sequence** **raster images of ones and zeros** – последователь-ность растровых изображений из единиц и нулей

**arranged in** - расположены в

**grid** - сетка, решетка

**represented using dots or squares** - представлены с исполь-зованием точек или квадратов

**variable** - переменная

**deliberate** - намеренный, обдуманный

**distinctive style** – отличительный (характерный) стиль

**to vary** - меняться

**predictable** - предсказуемый

**ray tracing** - трассировка лучей

**shading** - затемнение

**to depict** - отражать

**accurate and smooth surface patches** - точные и гладкие участки поверхности

**polygonal mesh modeling** - моделирование многоугольной сетки

Images are typically produced by optical devices; such as cameras, mirrors, lenses, telescopes, microscopes, etc. and natural objects and phenomena, such as the human eye or water surfaces.

A digital image is a representation of a two-dimensional image in binary format as a sequence of ones and zeros. Digital images include both vector images and raster images, but raster images are more commonly used.

**Pixel**

In the enlarged portion of the image individual pixels are rendered as squares and can be easily seen.

In digital imaging, a pixel (or picture element) is a single point in a raster image. Pixels are normally arranged in a regular 2-dimensional grid, and are often represented using dots or squares. Each pixel is a sample of an original image, where more samples typically provide a more accurate representation of the original. The intensity of each pixel is variable; in color systems, each pixel has typically three components such as red, green, and blue.

**Graphics**

Graphics are visual presentations on some surface, such as a wall, canvas, computer screen, paper, or stone to brand, inform, illustrate, or entertain. Examples are photographs, drawings, line art, graphs, diagrams, typography, numbers, symbols, geometric designs, maps, engineering drawings, or other images. Graphics often combine text, illustration, and color. Graphic design may consist of the deliberate selection, creation, or arrangement of typography alone, as in a brochure, flier, poster, web site, or book without any other element. Clarity or effective communication may be the objective, association with other cultural elements may be sought, or merely, the creation of a distinctive style.

**Rendering**

Rendering is the process of generating an image from a model (or models in what collectively could be called a scene file), by means of computer programs. A scene file contains objects in a strictly defined language or data structure; it would contain geometry, viewpoint, texture, lighting, and shading information as a description of the virtual scene. The data contained in the scene file is then passed to a rendering program to be processed and output to a digital image or raster graphics image file. The rendering program is usually built into the computer graphics software, though others are available as plug-ins or entirely separate programs. The term "rendering" may be by analogy with an "artist's rendering" of a scene. Though the technical details of rendering methods vary, the general challenges to overcome in producing a 2D image from a 3D representation stored in a scene file are outlined as the graphics pipeline along a rendering device, such as a GPU. A GPU is a purpose-built device able to assist a CPU in performing complex rendering calculations. If a scene is to look relatively realistic and predictable under virtual lighting, the rendering software should solve the rendering equation. The rendering equation does not account for all lighting phenomena, but is a general lighting model for computer-generated imagery. 'Rendering' is also used to describe the process of calculating effects in a video editing file to produce final video output.

**3D projection**

3D projection is a method of mapping three dimensional points to a two dimensional plane. As most current methods for displaying graphical data are based on planar two dimensional media, the use of this type of projection is widespread, especially in computer graphics, engineering and drafting.

**Ray tracing**

Ray tracing is a technique for generating an image by tracing the path of light through pixels in an image plane. The technique is capable of producing a very high degree of photorealism; usually higher than that of typical scanline rendering methods, but at a greater computational cost.

**Shading**

Shading refers to depicting depth in 3D models or illustrations by varying levels of darkness. It is a process used in drawing for depicting levels of darkness on paper by applying media more densely or with a darker shade for darker areas, and less densely or with a lighter shade for lighter areas. There are various techniques of shading including cross hatching where perpendicular lines of varying closeness are drawn in a grid pattern to shade an area. The closer the lines are together, the darker the area appears. Likewise, the farther apart the lines are, the lighter the area appears. The term has been recently generalized to mean that shaders are applied.

**Texture mapping**

Texture mapping is a method for adding detail, surface texture, or colour to a computer-generated graphic or 3D model. Its application to 3D graphics was pioneered by Dr. Edwin Catmull in 1974. A texture map is applied (mapped) to the surface of a shape, or polygon. This process is akin to applying patterned paper to a plain white box. Multitexturing is the use of more than one texture at a time on a polygon. Procedural textures (created from adjusting parameters of an underlying algorithm that produces an output texture), and bitmap textures (created in an image editing application or imported from a digital camera) are, generally speaking, common methods of implementing texture definition on 3D models in computer graphics software, while intended placement of textures onto a model's surface often requires a technique known as UV mapping (arbitrary, manual layout of texture coordinates) for polygon surfaces, while NURBS surfaces have their own intrinsic parameterization used as texture coordinates.

**3D modeling**

3D modeling is the process of developing a mathematical, wireframe representation of any three-dimensional object, called a "3D model", via specialized software. Models may be created automatically or manually; the manual modeling process of preparing geometric data for 3D computer graphics is similar to plastic arts such as sculpting. 3D models may be created using multiple approaches: use of NURBS curves to generate accurate and smooth surface patches, polygonal mesh modeling (manipulation of faceted geometry), or polygonal mesh subdivision (advanced tessellation of polygons, resulting in smooth surfaces similar to NURBS models). A 3D model can be displayed as a two-dimensional image through a process called 3D rendering, used in a computer simulation of physical phenomena, or animated directly for other purposes. The model can also be physically created using 3D Printing devices.

**Notes:**

**Pixel -** **Пиксель (пиксел) —** наименьший элемент изобра­жения или экрана в виде квадратика (квадратной точки), который может иметь индивидуальные параметры: яр­кость, цвет и др. Размер пикселя может быть разным в зави­симости от величины изображения и его разрешения, т. е. количества пикселов из которых оно состоит.

**GPU (Graphics Processing Unit)** - графический процессор. Он являет собой отдельное устройство игровой приставки, компьютера, фотоаппарата. Отвечает за рендеринг гра­фики, выполняет его.

**NURBS models -** Non-Uniform Rational B-Spline - неодно­родные рациональные B-сплайны. NURBS-кривые обла­дают одной особенностью: они всегда имеют гладкую форму.

**Rendering -** ре́ндеринг (англ. rendering — «визуализация») — термин в компьютерной графике, обозначающий про­цесс получения изображения по модели с помощью ком­пьютерной программы.

**Assignments**

**1. Translate the sentences from the texts into Russian in writing paying attention to the underlined words and phrases:**

1. A digital image is a representation of a two-dimensional image in binary format as a sequence of ones and zeros.
2. Digital images include both vector images and raster images, but raster images are more commonly used.
3. Graphic design may consist of the deliberate selection, creation, or arrangementof typography alone, as in a brochure, flier, poster, web site, or book without any other element.
4. 3D modeling is the process of developing a mathematical, wireframe representation of any three-dimensional object, called a "3D model", via specialized software.
5. Models may be created automatically or manually; the manual modeling process of preparing geometric data for 3D computer graphics is similar to plastic arts such as sculpting.

**2. Answer the following questions:**

1. What is the pixel`s representation?
2. What is the method of 3D projection?
3. Who was the pioneer of texture mapping?
4. What are the techniques of shading?
5. Give the description of 3D modeling process.

**3. Translate into English:**

Трёхмерная графика обычно имеет дело с виртуаль­ным, воображаемым трёхмерным пространством, которое отображается на плоской, двухмерной поверхности дис­плея или листа бумаги. В настоящее время известно не­сколько способов отображения трехмерной информации в объемном виде, хотя большинство из них представляет объёмные характеристики весьма условно, поскольку рабо­тают со стереоизображением. Из этой области можно отме­тить стереоочки, виртуальные шлемы, 3D-дисплеи, способ­ные демонстрировать трехмерное изображение. Несколько производителей продемонстрировали готовые к серийному производству трёхмерные дисплеи. Однако и 3D-дисплеи по-прежнему не позволяют создавать полноценной физи­ческой, осязаемой копии математической модели, созда­ваемой методами трехмерной графики.

**4. Give the summary of the text using the key terms.**

**IMAGE TYPES**

**Read the following words and word combinations and use them for understanding and translation of the text:**

**added semantic** value - добавленное семантическое значе-ние

**slight shift** - небольшое изменение

**to edit on the pixel level** - редактировать на пиксельном уровне

**to be complementary to** - дополнять

**to be akin to** – быть сродни чему-то

**relatively limited** - относительно ограничены

**instance** - случай, пример

**to rely on** - полагаться на что-то, зависеть от чего-то

**distinction** - различие, отличие

**keyframe** - ключевой кадр

**low bandwidth** - медленный канал

**virtual entities** - виртуальные объекты

**to be mapped** - отображаться

**Two-dimensional**

2D computer graphics are the computer-based generation of digital images — mostly from two-dimensional models, such as 2D geometric models, text, and digital images, and by techniques specific to them.

2D computer graphics are mainly used in applications that were originally developed upon traditional printing and drawing technologies, such as typography, cartography, technical drawing, advertising, etc. In those applications, the two-dimensional image is not just a representation of a real-world object, but an independent artifact with added semantic value; two-dimensional models are therefore preferred, because they give more direct control of the image than 3D computer graphics, whose approach is more akin to photography than to typography.

**Pixel art**

Pixel art is a form of digital art, created through the use of raster graphics software, where images are edited on the pixel level. Graphics in most old (or relatively limited) computer and video games, graphing calculator games, and many mobile phone games are mostly pixel art.

The term pixel art was first published by Adele Goldberg and Robert Flegal of Xerox Palo Alto Research Center in 1982. The concept, however, goes back about 10 years before that, for example in Richard Shoup's SuperPaint system in 1972, also at Xerox PARC.

Some traditional art forms, such as counted-thread embroidery (including cross-stitch) and some kinds of mosaic and beadwork, are very similar to pixel art. These art forms construct pictures out of small colored units similar to the pixels of modern digital computing. A similar concept on a much bigger scale can be seen in the North Korean Arirang Festival.

**Vector graphics**

Vector graphics formats are complementary to raster graphics. Raster graphics is the representation of images as an array of pixels and is typically used for the representation of photographic images. Vector graphics consists in encoding information about shapes and colors that comprise the image, which can allow for more flexibility in rendering. There are instances when working with vector tools and formats is best practice, and instances when working with raster tools and formats is best practice. There are times when both formats come together. An understanding of the advantages and limitations of each technology and the relationship between them is most likely to result in efficient and effective use of tools.

**Three-dimensional**

3D computer graphics in contrast to 2D computer graphics are graphics that use a three-dimensional representation of geometric data that is stored in the computer for the purposes of performing calculations and rendering 2D images. Such images may be for later display or for real-time viewing.

Despite these differences, 3D computer graphics rely on many of the same algorithms as 2D computer vector graphics in the wire frame model and 2D computer raster graphics in the final rendered display. In computer graphics software, the distinction between 2D and 3D is occasionally blurred; 2D applications may use 3D techniques to achieve effects such as lighting, and primarily 3D may use 2D rendering techniques.

3D computer graphics are often referred to as 3D models. Apart from the rendered graphic, the model is contained within the graphical data file. However, there are differences. A 3D model is the mathematical representation of any three-dimensional object. A model is not technically a graphic until it is visually displayed. Due to 3D printing, 3D models are not confined to virtual space. A model can be displayed visually as a two-dimensional image through a process called 3D rendering, or used in non-graphical computer simulations and calculations. There are some 3D computer graphics software for users to create 3D images e.g. Autocad, Photoshop, Solidwork, Google sketchup etc.

**Computer animation**

Computer animation is the art of creating moving images via the use of computers. It is a subfield of computer graphics and animation. Increasingly it is created by means of 3D computer graphics, though 2D computer graphics are still widely used for stylistic, low bandwidth, and faster real-time rendering needs. Sometimes the target of the animation is the computer itself, but sometimes the target is another medium, such as film. It is also referred to as CGI (Computer-generated imagery or computer-generated imaging), especially when used in films.

Virtual entities may contain and be controlled by assorted attributes, such as transform values (location, orientation, and scale) stored in an object's transformation matrix. Animation is the change of an attribute over time. Multiple methods of achieving animation exist; the rudimentary form is based on the creation and editing of keyframes, each storing a value at a given time, per attribute to be animated. The 2D/3D graphics software will interpolate between keyframes, creating an editable curve of a value mapped over time, resulting in animation. Other methods of animation include procedural and expression-based techniques: the former consolidates related elements of animated entities into sets of attributes, useful for creating particle effects and crowd simulations; the latter allows an evaluated result returned from a user-defined logical expression, coupled with mathematics, to automate animation in a predictable way (convenient for controlling bone behavior beyond what a hierarchy offers in skeletal system set up).

To create the illusion of movement, an image is displayed on the computer screen then quickly replaced by a new image that is similar to the previous image, but shifted slightly. This technique is identical to the illusion of movement in television and motion pictures.

**Notes:**

**Raster Graphics -** Компьютерное растровое изображение представляется в виде прямоугольной матрицы, каждая ячейка которой задана цветной точкой — вместе они фор­мируют целостную картинку. Пиксели подобны зернам фотографии и при значительном увеличении становятся заметными. Растровые изображения используются чаще векторных, так как они более просты в получении и допе­чатной подготовке.

**CGI (Computer-generated imagery or computer-generated imaging) -** стандарт интерфейса, используемого для связи внешней программы с веб-сервером. Программу, которая работает по такому интерфейсу совместно с веб-сервером, принято называть шлюзом, хотя многие предпочитают на­звания «скрипт» (сценарий) или «CGI-программа».

**CGI также может означать «Computer‐generated imagery» —** компьютерные спецэффекты.

**Assignments**

**1. Translate the sentences from the texts into Russian in writing paying attention to the underlined words and phrases:**

1. 2D computer graphics are mainly used in applications that were originally developed upon traditional printing and drawing technologies, such as typography, cartography, technical drawings.
2. Vector graphics formats are complementary to raster graphics.
3. Raster graphics is the representation of images as an array of pixels and is typically used for the representation of photographic images. g, advertising, etc.
4. Despite these differences, 3D computer graphics rely on many of the same algorithms as 2D computer vector graphics in the wire frame model and 2D computer raster graphics in the final rendered display.

**2. Answer the following questions:**

1. Where is 2D graphics traditionally used?
2. What do you know about pixel art?
3. What does vector graphics consist in?
4. What are the main differences between 2D and 3D graphics?
5. What methods of animation do you know?

**3. Translate into English:**

Компьютерная графика - технология создания и обра­ботки графических изображений средствами вычислитель­ной техники.

Компьютерная графика изучает методы получения изображений полученных на основании невизуальных данных или данных, созданных непосредственно пользова­телем.

Растровая графика (raster graphics) — вид компьютер­ной графики, используемой в приложениях, в частности, для рисования, близкого по технике к традиционному про­цессу (на бумаге или холсте). Данные в памяти ЭВМ хра­нятся в виде «карты» яркости и цвета для каждого элемента изображения (пикселя) или прямоугольной матрицы пик­селей (bitmap), дополненной данными о цвете и яркости каждого из них, а также способе сжатия записи и другими сведениями которые могут содержаться в «заголовке» и «концовке» файла.

Векторная графика (vector graphics) — вид компьютер­ной графики, используемой в приложениях для рисования. В отличие от растровой графики позволяет пользователю создавать и модифицировать исходные изобразительные образы при подготовке рисунков, технических чертежей и диаграмм путем их вращения, увеличения или уменьше­ния, растягивания. Графические образы создаются и хра­нятся в памяти ЭВМ в виде формул, описывающих различ­ные геометрические фигуры, которые являются компонен­тами изображения.

**4. Give the summary of the text using the key terms.**

**Topics for essays (you might need additional information):**

* History and development of computer graphics
* 3D modeling
* Computer animation

**ARTIFICIAL INTELLIGENCE: OVERVIEW**

**DEFINITIONS**

**Read the following words and word combinations and use them for understanding and translation of the text:**

**to impart** - наделять

**attribute** - определение

**highest good** – высшее благо

**offhand** – импровизированный, сделанный на скорую руку

**enclosed surface** – замкнутое пространство

**behavior pattern** – модель поведения

**observable** – наблюдаемый

**insufficient definition** – неполное определение

**tersely and concisely** – сжато и кратко

**to lose relevance** – терять актуальность

**human reasoning** – мышление человека, человеческое мыш-ление

**to adjust** – приспосабливаться

**productive approach** - плодотворный подход

**to a limited extent** – в определенных пределах

**chatterbot** – чатбот, программа «виртуальный собеседник»

The term *artificial intelligence* stirs emotions. For one thing there is our fascination with *intelligence*, which seemingly imparts to us humans a special place among life forms. Questions arise such as “What is intelligence?”, “How can one measure intelligence?” or “How does the brain work?” All these questions are meaningful when trying to understand artificial intelligence. However, the central question for the engineer, especially for the computer scientist, is the question of the intelligent machine that behaves like a person, showing intelligent behavior. The attribute *artificial* might awaken much different associations. It brings up fears of intelligent cyborgs. It recalls images from science fiction novels. It raises the question of whether our highest good, the soul, is something we should try to understand, model, or even reconstruct. With such different offhand interpretations, it becomes difficult to define the term *artificial intelligence* or *AI* simply and robustly.

In 1955, John McCarthy, one of the pioneers of AI, was the first to define the term *artificial* *intelligence*, roughly as follows: The goal of AI is to develop machines that behave as though they were intelligent.

To test this definition, imagine the following scenario. Fifteen or so small robotic vehicles are moving on an enclosed square surface. One can observe various behavior patterns. Some vehicles form small groups with relatively little movement. Others move peacefully through the space and gracefully avoid any collision. Still others appear to follow a leader. Aggressive behaviors are also observable. Is what we are seeing intelligent behavior? According to McCarthy’s definition these robots can be described as intelligent, thus it is clear that this definition is insufficient.

In the Encyclopedia Britannica one finds a definition that goes like: AI is the ability of digital computers or computer controlled robots to solve problems that are normally associated with the higher intellectual processing capabilities of humans . . . But this definition also has weaknesses. It would admit, for example, that a computer that can save a long text and retrieve it on demand displays intelligent capabilities, for memorization of long texts can certainly be considered a higher intellectual processing capability of humans, as can, for example, the quick multiplication of two 20-digit numbers. According to this definition, then, every computer is an AI system. This dilemma is solved elegantly by the following definition by Elaine Rich: Artificial Intelligence is the study of how to make computers do things at which, at the moment, people are better.

Rich, tersely and concisely, characterizes what AI researchers have been doing for the last 50 years. Even in the year 2050, this definition will be up to date.

Tasks such as the execution of many computations in a short amount of time are the strong points of digital computers. In this regard they outperform humans by many multiples. In many other areas, however, humans are far superior to machines. For instance, a person entering an unfamiliar room will recognize the surroundings within fractions of a second and, if necessary, just as swiftly make decisions and plan actions. To date, this task is too demanding for autonomous robots. According to Rich’s definition, this is, therefore, a task for AI. In fact, research on autonomous robots is an important, current theme in AI. Construction of chess computers, on the other hand, has lost relevance because they already play at or above the level of grandmasters.

It would be dangerous, however, to conclude from Rich’s definition that AI is only concerned with the pragmatic implementation of intelligent processes. Intelligent systems, in the sense of Rich’s definition, cannot be built without a deep understanding of human reasoning and intelligent action in general, because of which neuroscience is of great importance to AI. This also shows that the other cited definitions reflect important aspects of AI. A particular strength of human intelligence is adaptivity. We are capable of adjusting to various environmental conditions and change our behavior accordingly through *learning*. Precisely because our learning ability is so vastly superior to that of computers, *machine learning* is, according to Rich’s definition, a central subfield of AI.

In 1950, computer pioneer Alan M. Turing suggested a productive approach to evaluating claims of artificial intelligence in what became known as the Turing test. He gave a definition of an intelligent machine, in which the machine in question must pass the following test. The test person Alice sits in a locked room with two computer terminals. One terminal is connected to a machine, the other with a non-malicious person Bob. Alice can type questions into both terminals. She is given the task of deciding, after five minutes, which terminal belongs to the machine. The machine passes the test if it can trick Alice at least 30% of the time.

Computer programs have been able to pass the Turing test to a limited extent. The AI pioneer and social critic JosephWeizenbaum developed a program named Eliza, which is meant to answer a test subject’s questions like a human psychologist. He was in fact able to demonstrate success in many cases. Supposedly his secretary often had long discussions with the program. Today in the internet there are many so-called chatterbots, some of whose initial responses are quite impressive. After a certain amount of time, however, their artificial nature becomes apparent.

**Notes:**

**John McCarthy** (1927 - 2011) was a legendary computer scientist atStanford University who developed time-sharing, invented LISP, and founded the field of Artificial Intelligence.

**Elaine Rich** works as Distinguished Senior Lecturer at the University of Texas at Austin. Books: Automata, Computability and Complexity: Theory and Applications (author), Artificial Intelligence (co-author).

**Joseph Weizenbaum** (1923 - 2008) was a German-American computer scientist who is famous for his development of the Eliza program in 1966 and for his views on the ethics of artificial intelligence. He became sceptical of artificial intelligence and a leading critic of the AI field following the response of users to the Eliza program.

**Assignments**

**1. Translate the sentences from the texts into Russian in writing paying attention to the underlined words and phrases:**

1. The term *artificial intelligence* stirs emotions. For one thing there is our fascination with *intelligence*, which seemingly imparts to us humans a special place among life forms.
2. With such different offhand interpretations, it becomes difficult to define the term *artificial intelligence* or *AI* simply and robustly.
3. AI is the ability of digital computers or computer controlled robots to solve problems that are normally associated with the higher intellectual processing capabilities of humans.
4. In this regard they outperform humans by many multiples. In many other areas, however, humans are far superior to machines.
5. It would be dangerous, however, to conclude from Rich’s definition that AI is only concerned with the pragmatic implementation of intelligent processes.

**2. Answer the following questions:**

1. What is the key AI problem to be addressed by computer scientists?
2. Why is McCarthy’s definition called “insufficient”?
3. What is wrong with the definition of AI in the Encyclopedia Britannica?
4. Where do machines outperform humans? Where do people win?
5. What is the essence of the Turing test?

**3. Translate into English:**

Эрик Браун, 45-летний исследователь из IBM, отвечает за мозг суперкомпьютера *Ватсон*, который в 2011 г. получил известность победами над людьми в популярной телевик­торине. Самая большая трудность для Брауна, как настав­ника машины, не в том, чтобы впихнуть в Ватсона как можно больше знаний, но в том, чтобы придать тонкость его пониманию языка. Например, научить слэнгу.

Как проверить, может ли компьютер «мыслить»? Клас­сический тест — так называемый тест Тьюринга — прост: он предполагает способность вести светскую беседу. Если бы компьютер сумел бы не выдать свою двоичную сущ­ность в непринужденном разговоре, он бы доказал свое ин­теллектуальное превосходство. Но пока ни одной машине это не удалось.

Два года назад Браун попытался натаскать Ватсона с помощью популярного веб-сайта Urban Dictionary. Словар­ные статьи на сайте составляются обычными пользовате­лями и редактируются добровольными редакторами по достаточно произвольным правилам. Тут есть всевозмож­ные актуальные аббревиатуры как bb (англ. bye bye) — пока, hf (англ. have fun) — отлично повеселиться, w8 (англ. wait) — жди. В том числе и огромное количество всяких слэнговых конструкций, таких, как hot mess — «горячая штучка».

Но Ватсон не мог различить салонную лексику и слэн­говую — которой в Urban Dictionary хватает. Кроме того, из-за чтения Википедии Ватсон приобрел некоторые дурные привычки. В ответах на вопросы исследователя в тестах он использовал малоцензурные словечки.

В конечном счете команда Брауна разработала фильтр, чтобы отцеживать брань Ватсона, и выскребла Urban Dictionary из его памяти. Это испытание доказывает, на­сколько тернист будет путь любого железного интеллек­туала к “лёгкой болтовне”. Теперь Браун подготавливает Ватсона к использованию в качестве диагностического ин­струмента в больнице: там знание всяких модных аббре­виатур не потребуется.

**4. Give the summary of the text using the key terms.**

**APPROACHES AND TECHNIQUES**

**Read the following words and word combinations and use them for understanding and translation of the text:**

**conventional** - общепринятый, традиционный

**computational intelligence** - вычислительный интеллект **machine learning** - машинное обучение

**case-based reasoning** - вывод (рассуждения), основанные на прецедентах

**behavior-based AI** - поведенческий ИИ

**referred to as** - под названием, именуемый

**neural networks** - нейронные сети

**fuzzy logic** - нечеткая логика

**neats versus scruffies** - чистюли против нерях

**ad hoc rules** - ситуативные правила

**inference engine** - механизм логического вывода

**forward chaining** - прямой логический вывод

**backward chaining** - обратный логический вывод

**directed acyclic graph** - ориентированный циклический граф

**arc** - дуга

**conditional dependence** - условная зависимость

**to be subject to controversy** - вызывать споры

**track record** - послужной список, достижения

The artificial intelligence community can be roughly divided into two schools of thought: conventional AI and computational intelligence. *Conventional AI* is based on machine learning, which is the development of the techniques and algorithms that allow machines to “learn” or at least simulate learning. Machine learning attempts to use computer programs to generate patterns or rules from large data sets. This problem is similar to the data-mining problem (and data mining is one area where AI has found commercial success). Machine learning makes heavy use of symbolic formalism and logic, as well as statistics. Key areas in conventional AI include case-based reasoning, behavior-based AI, Bayesian networks, and expert systems. *Computational intelligence*, in contrast, relies more on clever algorithms (heuristics) and computation and less on formal logical systems. Computational intelligence is sometimes referred to as soft computing. It often involves iterative methods using computation to generate intelligent agents. Whereas conventional AI is considered to be a *top-down approach*, with the structure of solutions imposed from above, computational intelligence is more *bottom-up*, where solutions emerge from an unstructured initial state. Two areas of computational intelligence will be discussed further: neural networks and fuzzy logic. Hybrid intelligent systems attempt to combine the two approaches. Some proponents claim that this is appropriate, because the human mind uses multiple techniques to develop and verify results, and hybrid systems show some promise.

Another distinction within the artificial intelligence community is *weak AI* versus *strong AI*. Weak AI refers to using software to solve particular problems or reasoning tasks that do not encompass fully human intelligence. Strong AI implies creating artificial systems that are fully self-aware, the systems that can reason and independently solve problems. Current research is nowhere near creating strong AI, and a lively debate is ongoing as to whether this is even possible.

Another division in the artificial intelligence community is over the best way to design an intelligent system (*Neats* versus *Scruffies*). The Neats maintain that the solution should be elegant, obvious, and based on formal logic. The Scruffies hold that intelligence is too messy and complicated to be solved under the limitations the Neats propose. Interestingly, some good results have come from hybrid approaches, such as putting ad hoc rules (Scruffy style) into a formal (Neat) system. Not surprisingly, the Neats are often associated with conventional artificial intelligence, whereas the Scruffies are usually associated with computational intelligence.

Conventional AI has achieved success in several areas. **Expert systems**, or knowledge-based systems, attempt to capture the domain expertise of one or more humans and apply that knowledge. Most commonly, this is done by developing a set of rules that analyze information about a problem and recommend a course of action. Expert systems demonstrate behavior that appears to show reasoning. Expert systems work best in organizations with high levels of know-how and expertise that are difficult to transfer among staff. The simpler expert systems are all based on binary logic, but more sophisticated systems can include methods such as fuzzy logic. At the heart of an expert system is an *inference engin*e, a program that attempts to create answers from the *knowledge base* of rules provided by the expert. Knowledge engineers convert a human expert’s “rules-of-thumb” into inference rules, which are if-then statements that provide an action or a suggestion if a particular statement is true. The inference engine then uses these inference rules to reason out a solution. *Forward chaining* starts with the available information and tries to use the inference rules to generate more data until a solution is reached. *Backward-chaining* starts with a list of solutions and works backward to see if data exists that will allow it to conclude that any of the solutions are true. Expert systems are used in many fields, including finance, medicine, and automated manufacturing.

Another approach from conventional AI that has achieved some commercial success is **case-based reasoning**, or CBR, which attempts to solve new problems based on past solutions of similar problems. Proponents argue that case-based reasoning is a critical element in human problem solving. As formalized in computer reasoning, CBR is composed of four steps: retrieve, reuse, revise, retain. First, access the available information about the problem (Retrieve). Second, try to extend a previous solution to the current problem (Reuse). Next, test the refactored solution and revise it if necessary (Revise). Finally, store the new experience into the knowledge base (Retain).

**Behavior-based artificial intelligence (BBAI)** attempts to decompose intelligence into a set of distinct, semi-autonomous modules. BBAI is popular in the robotics field and is the basis for many Robocup robotic soccer teams, as well as the Sony Aibo. A BBAI system is composed of numerous simple behavior modules, which are organized into layers. Each layer represents a particular goal of the system, and the layers are organized hierarchically. A low layer might have a goal of “avoid falling,” whereas the layer above it might be “move forward.” The move forward layer might be one component of a larger “walk to the store” goal. The layers can access sensor data and send commands to the robot’s motors. The lower layers tend to function as reflexes, whereas the higher layers control more complex goal-directed behavior.

**Bayesian networks** are another tool in the conventional AI approach. They are heavily based upon probability theory. The problem domain is represented as a network. This network is a directed acyclic graph where the nodes represent variables, and the arcs represent conditional dependences between the variables. Graphs are easy to work with, so Bayesian networks can be used to produce models that are simple for humans to understand, as well as effective algorithms for inference and learning. Bayesian networks have been successfully applied to numerous areas, including medicine, decision support systems, and text analysis, including optical character recognition.

There is no widespread agreement yet on exactly what Computational intelligence (CI) is, but it is agreed that it includes **neural networks** and **fuzzy computing**. A **neural network** consists of many nodes that cooperate to produce an output. The system is trained by supplying input on the solution of known problems, which changes the weighting between the nodes. After training has tuned the parameters between the connections, neural networks can solve difficult problems in machine vision and other areas. Also known as neurocomputing, or parallel distributed processing, neural networks loosely model structures in the human brain. Neural network outputs rely on the cooperation of individual nodes. Data processing in neural networks is typically done in parallel, rather than sequentially as is the standard for nearly all modern computers. Neural nets can generalize from their training, and solve new problems, so they are self-adaptive systems. Neural networks have been criticized as “bad science” because it is difficult to explain exactly how they work. Nonetheless, neural networks have been successfully applied in areas as diverse as credit card fraud detection, machine vision, chess, and vehicle control.

**Fuzzy logic**, fuzzy systems, and fuzzy set theory are all ways to refer to reasoning that is based upon approximate values, rather than precise quantities. Modern computers are built upon binary, or Boolean, logic that is based on ones and zeros. The bit is zero or one, yes or no, with no middle ground. Fuzzy systems provide for a broader range of possible values. Consider the question, “Are the books in the study?” Well, yes, there are books in the study. There are also books in the office, books in the bedroom, and a pile of books in the doorway to the study. Fuzzy logic provides for an answer of 72%, meaning that 72% of the books are in the study. Fuzzy sets are based on vague definitions of sets. They are not random. Fuzzy logic is not imprecise; rather, it is a formal mathematical technique for handling imprecise data. Like neural networks, fuzzy logic is subject to controversy and criticism. But systems based on fuzzy logic have an excellent track record at certain types of problems. Antilock braking systems are based on fuzzy logic, and many appliances incorporate fuzzy logic.

**Notes:**

**Bayesian network** (Bayesian network, Bayes network, belief network, Bayes(ian) model or probabilistic directed acyclic graphical model) is aprobabilistic graphical model (a type of statistical model) that represents a set of random variables and their conditional dependencies via a directed acyclic graph (DAG).

**Robocup** is an international robotics competition that aims to develop autonomous robots with the intention of developing research and education in the field of artificial intelligence. The best universities in the world compete in several leagues.

**AIBO** (Artificial Intelligence robot) is a robotic project from Sony. In Japanese, AIBO means pal or partner. AIBO was one of several types of robotic pets that were designed and manufactured by Sony. **Sony Aibo** is basically a robotic dog that that is able to walk and “see” its environment using the on board cameras. It is even able to recognize spoken commands in languages including Spanish and English.

**Assignments**

**1. Translate the sentences from the texts into Russian in writing paying attention to the underlined words and phrases:**

1. Machine learning makes heavy use of symbolic formalism and logic, as well as statistics.
2. Whereas conventional AI is considered to be a *top-down approach*, with the structure of solutions imposed from above, computational intelligence is more *bottom-up*, where solutions emerge from an unstructured initial state.
3. Some proponents claim that this is appropriate, because the human mind uses multiple techniques to develop and verify results, and hybrid systems show some promise.
4. Weak AI refers to using software to solve particular problems or reasoning tasks that do not encompass fully human intelligence.
5. Current research is nowhere near creating strong AI, and a lively debate is ongoing as to whether this is even possible.
6. The Neats maintain that the solution should be elegant, obvious, and based on formal logic. The Scruffies hold that intelligence is too messy and complicated to be solved under the limitations the Neats propose.
7. Expert systems, or knowledge-based systems, attempt to capture the domain expertise of one or more humans and apply that knowledge.
8. There is no widespread agreement yet on exactly what Computational intelligence (CI) is, but it is agreed that it includes neural networks and fuzzy computing.

**2. Answer the following questions:**

1. What are the ways to classify Artificial Intelligence?
2. How does an expert system work?
3. What are the four steps in case-based reasoning?
4. What tasks do the layers of a BBAI system perform?
5. Where are Bayesian networks applied?
6. What are the working principles of a neural network?
7. How does fuzzy logic differ from Boolean logic?

**3. Translate into English:**

Эпименид Кносский с острова Крит – полумифический поэт и философ, живший в VI в. до н.э., однажды заявил: «Все критяне – лжецы!». Так как он и сам был критянином, то его помнят как изобретателя так называемого критского парадокса.

В терминах аристотелевой логики, в которой утвер­ждение не может быть одновременно истинным и ложным, и подобные самоотрицания не имеют смысла. Если они ис­тинны, то они ложны, но если они ложны, то они истинны.

И здесь на сцену выходит нечеткая логика, где пере­менные могут быть частичными членами множеств. Ис­тинность или ложность перестают быть абсолютными – ут­верждения могут быть частично истинными и частично ложными. Использование подобного подхода позволяет строго математически доказать, что парадокс Эпименида ровно на 50% истинен и на 50% ложен.

Таким образом, нечеткая логика в самой своей основе несовместима с аристотелевой логикой, особенно в отно­шении закона Tertium non datur («Третьего не дано» – лат.), который также называют *законом исключения среднего*. Если сформулировать его кратко, то звучит он так: если утвер­ждение не является истинным, то оно является ложным. Эти постулаты настолько базовые, что их часто просто принимают на веру.

Более банальный пример пользы нечеткой логики можно привести в контексте концепции холода. Большин­ство людей способно ответить на вопрос: «Холодно ли вам сейчас?». В большинстве случаев люди понимают, что речь не идет об абсолютной температуре по шкале Кельвина. Хотя температуру в 0 K можно, без сомнения, назвать холо­дом, но температуру в +15 C многие холодом считать не будут.

Но машины не способны проводить такую тонкую гра­дацию. Если стандартом определения холода будет «тем­пература ниже +15 C», то +14,99 C будет расцениваться как холод, а +15 C – не будет!

**4. Give the summary of the text using the key terms.**

**CURRENT TRENDS**

**Read the following words and word combinations and use them for understanding and translation of the text:**

**hype** - навязчивая (агрессивная) реклама, рекламная шу-миха, раскрутка

**acquisitions** - приобретение

**buzz word** - модное словцо

**cognitive computing** - когнитивные вычисления, познава-тельные вычисления

**predictive analytics** - прогнозная аналитика

**two-voice counterpoint** - двухголосая полифония (контра-пункт)

**visual cue** - визуальная подсказка

**to underpin** - лежать в основе

**big data** - большие данные, супермассив данных

**to sift through** - перелопатить

**evidence** - реальные факты, полученные сведения

**to leverage** - выгодно использовать, по-новому применять

**relevant information** - необходимая (актуальная) информация

It looks like the beginning of a new technology hype for artificial intelligence (AI). The media has started flooding the news with product announcements, acquisitions, and investments. AI is capturing the attention of tech firm and investor giants such as Google, Microsoft, and IBM. The buzz words are great too: cognitive computing, deep learning, AI2.

For those who started their careers in AI and left in disillusionment or data scientists today, the consensus is often that artificial intelligence is just a new fancy marketing term for good old predictive analytics.They point to the reality of Apple’s Siri to listen and respond to requests as adequate but more often frustrating. Or, IBM Watson’s win on Jeopardy as data loading and brute force programming.

But, is this fair? No. New AI breaks the current rule that machines must be better than humans: they must be smarter, faster analysts, or manufacture things better and cheaper.

New AI says:

* *The question is sometimes more important than the answer*. Suggestions don’t always need to be answers, they can be questions. Eric Horvitz of Microsoft told MIT Technology Review, “…Another possibility is to build systems that understand the value of information, meaning they can automatically compute what the next best question to ask is....”
* *Improvisation is the true meaning of adaptation.* Search on ‘artificial intelligence’ and ‘improvisation’ and you get a lot of examples of AI being linked to music. The head of Facebook’s AI lab and musician, Yan Lecun, says,“I have always been interested in Jazz because I have always been intrigued by the intellectual challenge of improvising music in real time”. Linking the two, he wrote a program that automatically composed two-voice counterpoint for a college artificial intelligence project.
* *Collaboration produces better results.* Guy Hoffman at the Media Innovation Lab, School of Communication, IDC Herzliya introduced a robot that could not only compose music independently, but also collaborate with another musician (Guy himself) to create a new piece of music. The robot provided visual cues, reacting and communicating the effect of the music and creative process for lifelike interaction between robot and composer.

This is game changing, both in how organizations operate and strategize as well as the impact on customer experience. These three principles are the foundation for customer and organizational engagement. Today AI is like a super smart magic eight ball. Tomorrow AI supports and creates a dialog between companies and customers, managers and employees, and business to business.

We’re now seeing the emergence of [**cognitive computing**](http:///h), a new era of computing systems that will understand the world in the way that humans do: through senses, learning, and experience.

These new cognitive systems will help us think. They will relate to us and answer questions using the language we humans use every day. They will learn from their interactions with data and with us, basically adapting their behavior automatically based on new knowledge.

That’s what makes this third major era of computing such a huge leap forward. The first era was made up of tabulating machines and the second of programmable computers. While the programmable era will continue perhaps indefinitely and certainly underpin the next era of computing,cognitive systems represent a whole new approach to solving complex data and information analysis problems that goes beyond just computing.

Data is available everywhere, all the time. It’s piling up, simply waiting to be used. Which is why we need computing systems that we can interact with using human language, rather than programming language. We need computers that can dish up advice, rather than waiting for commands.

How will these systems work? IBM Watson, one of the first systems built as a cognitive computing system, applies deep analytics to text and other unstructured big data sources to pull meaning out of the data by using inference, probability, and reasoning to solve complex problems. Watson is a first step toward cognitive computing, expanding the reaches of human understanding by helping us quickly and efficiently sift through massive amounts of data, pinpointing the information and insights that are now trapped within these sources.

Watson does this by using hundreds of analytics, which provide it with capabilities such as natural language processing, text analysis, and knowledge representation and reasoning to make sense of huge amounts of complex information in split seconds, rank answers based on evidence and confidence, and learn from its mistakes. And, of course, this capability is deployed in the [cloud](http:///h) and made available to applications as a cognitive service.

One of the first domains for Watson is healthcare. Cleveland Clinic is working to explore how Watson can be used to better leverage valuable information trapped in large electronic health records. Watson’s analytics can sift through unstructured clinical notes in a patient’s health record, reason over that information, and connect it with other structured information in the health record to produce summaries, deeper insights, and faster access to relevant information.

A new application of Watson, called WatsonPaths, is able to analyze complex medical scenarios and propose relationships and connections to possible diagnoses extracted from the underlying medical literature. Medical students can interact with WatsonPaths to both learn from Watson and teach Watson by grading Watson’s recommendations.

"Right now the science of cognitive computing is in the formative stages," says IBM Research's Ton Engbersen. "To become machines that can learn, computers must be able to process sensory as well as transactional input, handle uncertainty, draw inferences from their experience, modify conclusions according to feedback, and interact with people in a natural, human-like way."

Watson is a first step, but it points to what will be possible and how the age of cognitive computing will transform how we work with computers and what we expect out of them, helping remake our industries, economies and societies.

**Notes:**

**deep learning** is a set of algorithms in machine learning that attempt to model high-level abstractions in data by using architectures composed of multiple non-linear transformations.[[](http://en.wikipedia.org/wiki/Deep_learning#/h)

**brute force programming** - программирование методом "грубой силы", неэффективный с точки зрения расходова­ния вычислительных ресурсов стиль программирования, решение "в лоб", когда программист полагается только на производительность компьютера, вместо того чтобы попы­таться упростить задачу, - поэтому программы получаются громоздкими, тяжеловесными, неэлегантными. В ряде слу­чаев такой подход оправдан, например, когда решение ра­зовой задачи нужно получить любой ценой

**magic eight ball** также **mystic 8 ball**, **шар судьбы**, **шар во­просов и ответов**, **шар предсказаний** — игрушка, шуточ­ный способ предсказывать будущее. Это шар, сделанный из пластмассы, обычно диаметром 10-11 см, внутри которого есть емкость с тёмной жидкостью, в которой плавает фи­гура с 20 поверхностями — икосаэдр, на которых нанесены ответы. Ответы (20 вариантов) нанесены в формате «да», «нет», «абсолютно точно», «плохие шансы», «вопрос не ясен», и т. д.

**Assignments**

**1. Translate the sentences from the texts into Russian in writing paying attention to the underlined words and phrases:**

* For those who started their careers in AI and left in disillusionment or data scientists today, the consensus is often that artificial intelligence is just a new fancy marketing term for good old predictive analytics.
* This is game changing, both in how organizations operate and strategize as well as the impact on customer experience. These three principles are the foundation for customer and organizational engagement.
* While the programmable era will continue perhaps indefinitely and certainly underpin the next era of computing,cognitive systems represent a whole new approach to solving complex data and information analysis problems that goes beyond just computing.
* Watson is a first step toward cognitive computing, expanding the reaches of human understanding by helping us quickly and efficiently sift through massive amounts of data, pinpointing the information and insights that are now trapped within these sources.

**2. Answer the following questions:**

1. What is the current situation in the field of AI?
2. What are the three basic principles of new AI?
3. Why is AI (in its current state) called “a super smart magic eight ball”?
4. How does Watson address complex problems?
5. Where can cognitive computing systems be applied?

**3. Translate into English:**

До сих пор все, что было в кибернетике и вычисли­тельной технике, базировалось, так или иначе, на моделях фон Неймана и Тьюринга. Сегодня IBM Research исследует следующее поколение вычислительных систем — *когни­тивных* — они, по сути, отходят от модели Тьюринга, кото­рая говорит о том, что любое вычисление может быть пред­ставлено в виде бесконечной ленты ячеек, в каждой из ко­торых находится одна простая команда.

Человеческий мозг так не работает. У нейронов, во-первых, гораздо больше связей; во-вторых, у нервной клетки больше состояний, чем 0 и 1. А в-третьих, и это са­мое важное, у традиционных кибернетических устройств есть 3 принципиально разные функции, разделенные ме­жду разными модулями. Одна функция — это память, где хранится информация, вторая функция — это устройство ввода-вывода и третья — это, собственно говоря, функция вычисления. Нейрон – устройство универсальное: он полу­чает информацию, хранит и перерабатывает ее.

Таким образом, когнитивные машины, конечно, должны не заново создавать мозг (природа один раз уже это сделала), а на основе тех знаний о физических и химиче­ских процессах, которые происходят в чипе, попытаться воспроизвести этот единый, параллельный по природе, растянутый во времени процесс познания, мышления, вос­приятия и осмысления реальности, и на этом основании выдать решение.

Пока что живые системы гораздо более эффективны, прежде всего, энергетически. Суперкомпьютер Watson**,** обыгравший участников телевикторины Jeopardy!, потреб­ляет 80 кВт энергии, а человеческий мозг — 20 Вт. То есть Watson в 4 тыс. раз менее энергоэффективен, чем мозг: на одинаковое по результату действие у него уходит гораздо больше энергии, чем у человека.

**4. Give the summary of the text using the key terms.**

**Topics for essays (you might need additional information):**

* The origins of AI
* Expert systems
* AI2
* Cognitive computing

**ARTIFICIAL INTELLIGENCE: ROBOTICS AND A-LIFE**

**ROBOTICS**

**Read the following words and word combinations and use them for understanding and translation of the text:**

**intricate** - мудреный, замысловатый, сложный

**gears and cams** - шестеренки и эксцентрики

**tentative** - пробный, экспериментальный

**serf** - крепостной

**end effector** - рабочий орган, захватное устройство, кольце-вой захват

**welding** - сварка, сварочные работы

**automatic guided vehicle** - робокар, автоматически управляемая тележка

**scouting** - разведка, дозор

**rover** - самоходная машина

**law enforcement** - правоохранительные органы, охрана пра-вопорядка

**market penetration** - внедрение (выход) на рынок

**low-wage** - низкооплачиваемый

**hazardous materials** - опасные вещества

**viability** - жизнеспособность, живучесть

**swarm intelligence** - роевой интеллект

**swarm robotics** - групповая робототехника

**fault tolerance** - отказоустойчивость

**malfunction** - сбой, неисправность

**scalable** - масштабируемый, размерно варьируемый

**mapping** - картографирование

**senior lecturer** - старший преподаватель

**search-and-rescue** - поисково-спасательный

**contaminated environment** - зараженная окружающая среда

**envision** - предвидеть, представлять себе, воображать

The idea of the automaton — the lifelike machine that performs intricate tasks by itself — is very old. Simple automatons were known to the ancient world. By the 18th century, royal courts were being entertained by intricate humanlike automatons that could play music, draw pictures, or dance. A little later came the “Turk,” a chess-playing automaton that could beat most human players.

However, things are not always what they seem. The true automatons, controlled by gears and cams, could play only whatever actions had been designed into them. They could not be reprogrammed and did not respond to changes in their environment. The chess-playing automaton held a concealed human player. True robotics began in the mid-20th century and has continued to move between two poles: the pedestrian but useful industrial robots and the intriguing but tentative creations of the artificial intelligence laboratories.

**Industrial Robots**

In 1921, the Czech playwright Karel Capek wrote a play called *R.U.R.* or *Rossum’s Universal Robots.* Robot is a Czech word that has been translated as work(er), serf, or slave. In the play the robots, which are built by factories to work in other factories, eventually revolt against their human masters. During the 1960s, real robots began to appear in factory settings.

An industrial robot is basically a movable arm that ends in a “hand” called an end effector. The arm and hand can be moved by some combination of hydraulic, pneumatic, electrical, or mechanical means. Typical applications include assembling parts, welding, and painting. The robot is programmed for a task either by giving it a detailed set of commands to move to, grasp, and manipulate objects, or by “training” the robot by moving its arm, hand, and effectors through the required motions, which are then stored in the robot’s memory. The early industrial robots had very little ability to respond to variations in the environment, such as the “work piece” that the robot was supposed to grasp being slightly out of position. However, later models have more sophisticated sensors to enable them to adjust to variations and still accomplish the task.

**Mobile Robots and Service Robots**

Industrial robots work in an extremely restricted environment, so their world representation can be quite simple. However, robots that can move about in the environment have also been developed. Military programs have developed automatic guided vehicles (AGVs) with wheels or tracks, capable of navigating a battlefield and scouting or attacking the enemy. Space-going robots including the Sojourner Mars rover also have considerable onboard “intelligence,” although their overall tasks are programmed by remote commands.

Indeed, the extent to which mobile robots are truly autonomous varies considerably. At one end is the “robot” that is steered and otherwise controlled by its human operator, such as law enforcement robots that can be sent into dangerous hostage situations.

Moving toward greater autonomy, we have the “service robots” that have begun to show up in some institutions such as hospitals and laboratories. These mobile robots are often used to deliver supplies. For example, the Help-Mate robot can travel around a hospital by itself, navigating using an internal map. It can even take an elevator to go to another floor.

Service robots have had only modest market penetration, however. They are relatively expensive and limited in function, and if relatively low-wage more versatile human labor is available, it is generally preferred. For now mobile robots and service robots are most likely to turn up in specialized applications in environments too dangerous for human workers, such as in the military, law enforcement, handling of hazardous materials, and so on.

**Smart Robots**

Robotics has always had great fascination for artificial intelligence researchers. After all, the ability to function convincingly in a real-world environment would go a long way toward demonstrating the viability of true artificial intelligence. Building a smart, more humanlike robot involves several interrelated challenges, all quite difficult. These include developing a system for seeing and interpreting the environment (computer vision) as well a way to represent the environment internally so as to be able to navigate around obstacles and perform tasks.

One of the earliest AI robots was “Shakey,” built at the Stanford Research Institute (SRI) in 1969. Shakey could navigate only in a rather simplified environment. However, the “Stanford Cart,” built by Hans Moravec in the late 1970s could navigate around the nearby campus without getting into too much trouble.

An innovative line of research began in the 1990s at MIT. Instead of a “top down” approach of programming robots with explicit logical rules, so-called behavior-based robotics works from the bottom up, coupling systems of sensors and actuators that each have their own simple rules, from which can emerge surprisingly complex behavior. The MIT “sociable robots” Cog and Kismet were able to explore the world and learn to interact with people in somewhat the way a human toddler might.

**Swarm robotics** is an approach to robotics that emphasizes many simple robots instead of a single complex robot. A robot swarm has much in common with an ant colony or swarm of bees. No individual in the group is very intelligent or complex, but combined, they can perform difficult tasks. Swarm robotics has been an experimental field, but many practical applications have been proposed.

A traditional robot often needs complex components and significant computer processing power to accomplish its assigned tasks. In swarm robotics, each robot is relatively simple and inexpensive. As a group, these simple machines cooperate to perform advanced tasks that otherwise would require a more powerful, more expensive robot.

Using many simple robots has other advantages as well. Robot swarms have high fault tolerance, meaning that they still will perform well if some of the individual units malfunction or are destroyed. Swarms also are scalable, so the size of the swarm can be increased or decreased as needed.

One use that researchers have demonstrated for swarm robotics is mapping. A single robot would constantly need to keep track of its location, remember where it had been and figure out how to avoid obstacles while still exploring the entire area. A swarm of robots could be programmed simply to avoid obstacles while keeping in contact with other members of the swarm. The data from all of the robots in the swarm is then combined into a single map.

Swarm robotics has been an emerging field, and it has presented unique challenges to researchers. Programming a swarm of robots is unlike other types of programming. The model of distributed computing — using many computers to work on a single large task — is somewhat similar. Unlike distributed computing, however, each individual in swarm-style robotics deals with unique stimuli. Each robot, for example, is in a different location at any given time.

Some approaches to swarm robotics use a control unit that coordinates other robots. Other approaches use techniques borrowed from nature to give the swarm itself a type of collective intelligence. Much of the current research in the field focuses on finding the most efficient way to use a swarm.

Swarm robotics is a concept that's buzzed around since the 1980s, but now the technology is starting to fly. The environmental applications being explored range from coral restoration and oil spill clean-ups to precision farming – even the creation of artificial bees to pollinate crops.

Dr Roderich Gross, senior lecturer in robotics and computational intelligence, explains the concept: "In a swarm system there is no single point of failure – if a unit fails, the whole system keeps on going. Wherever you have a very heavy load that a human cannot manipulate, using a swarm of robots to do the job would be very sensible. That could be in a factory, transporting boxes. Or it could be a search-and-rescue scenario – maybe a collapsed building and you need to remove a very heavy part, or working in contaminated environments."

Scientists and designers at Heriot-Watt University have been looking at using a swarm of "coral bots" to restore ocean habitats. Dr Lea-Anne Henry of the university's school of life sciences believes that swarm robotics can "revolutionise conservation"*.* Agriculture is looking into the potential for using swarms too. Professor Simon Blackmore, head of engineering at Harper Adams University works on larger robots that can work in fleets, able to identify weeds and administer microdots of chemicals with the result of using 99.9% less herbicide than traditional methods. He believes that, though the technology may appear an expensive luxury, it may have a wider appeal than the latest generation of conventional farm machinery such as expensive tractors and harvesters.

Perhaps the most famous – and controversial – swarm project to date is Harvard University's "Robobees", aiming to find an artificial solution to pollination to address the current decline in the global bee population. Here the robotic swarm is attempting to replicate one of nature's greatest swarms. But even setting aside the ethics of attempting to replace nature's pollinators, the idea may remain impossible.

The problems of organizing a swarm haven’t kept people from imagining what swarm robotics could offer some day. Some scientists envision a swarm of very small microbots being used to explore other planets. Other proposed uses include search-and-rescue missions, mining and even firefighting. When used with nanobots — microscopic-size robots — swarm robotics could even be used in human medicine.

**Future Applications**

A true humanoid robot with the kind of capabilities written about by Isaac Asimov and other science fiction writers is not in sight yet. However, there are many interesting applications of robots that are being explored today. These include the use of remote robots for such tasks as performing surgery (telepresence) and the application of robotics principles to the design of better prosthetic arms and legs for humans (bionics). Farther afield is the possibility of creating artificial robotic “life” that can self-reproduce.

**Notes:**

**The Turk**, also known as the **Mechanical Turk** or **Automaton Chess Player** was a fake chess-playing machine constructed in the late 18th century. From 1770 until its destruction by fire in 1854, it was exhibited by various owners as an automaton, though it was exposed in the early 1820s as an elaborate hoax.

**Karel Čapek** (1890 – 1938) was a Czech writer of the early 20th century best known for his science fiction, including his novel *War with the Newts* and the play *R.U.R.* that introduced the word *robot*.

**Sojourner** was the [Ma](http:///h)rs Pathfinder robotic Mars rover that landed on July 4, 1997 and explored Mars for around three months.

**Shakey the robot** was the first general-purpose mobile robot to be able to reason about its own actions. While other robots would have to be instructed on each individual step of completing a larger task, Shakey could analyze the command and break it down into basic chunks by itself. It was developed from approximately 1966 through 1972 at the Artificial Intelligence Center of Stanford Research Institute

**MIT (Massachusetts Institute of Technology**) is a [priv](http:///h)a[te](http:///h) research university in Cambridge, Massachusetts, founded in 1861 in response to the increasing [industrializ](http:///h)ation of the United States. The institute adopted apolytechnic university model and stressed laboratory instruction.

**RoboBee** is a tiny robot capable of tethered flight, developed by a research robotics team at Harvard University. The 3-centimeter (1.2 in) wingspan of RoboBee makes it the smallest man-made device modeled on an insect to achieve flight.

**Assignments**

**1. Translate the sentences from the texts into Russian in writing paying attention to the underlined words and phrases:**

1. True robotics began in the mid-20th century and has continued to move between two poles: the pedestrian but useful industrial robots and the intriguing but tentative creations of the artificial intelligence laboratories.
2. The early industrial robots had very little ability to respond to variations in the environment, such as the “work piece” that the robot was supposed to grasp being slightly out of position.
3. At one end is the “robot” that is steered and otherwise controlled by its human operator, such as law enforcement robots that can be sent into dangerous hostage situations.
4. Service robots have had only modest market penetration, however.
5. After all, the ability to function convincingly in a real-world environment would go a long way toward demonstrating the viability of true artificial intelligence.
6. Swarm robotics has been an emerging field, and it has presented unique challenges to researchers.
7. Other approaches use techniques borrowed from nature to give the swarm itself a type of collective intelligence.
8. Swarm robotics is a concept that's buzzed around since the 1980s, but now the technology is starting to fly.
9. He believes that, though the technology may appear an expensive luxury, it may have a wider appeal than the latest generation of conventional farm machinery such as expensive tractors and harvesters.
10. Perhaps the most famous – and controversial – swarm project to date is Harvard University's "Robobees", aiming to find an artificial solution to pollination to address the current decline in the global bee population.

**2. Answer the following questions:**

1. How was the term “robot” coined?
2. What are the limitations of industrial robots?
3. Where are mobile robots being used?
4. What approaches does the development of smart robots call for?
5. What are the advantages of swarm robotics over conventional approaches?
6. What are the major challenges posed by swarm robotics?
7. Where can swarm intelligence be of practical assistance?

**3. Translate into English:**

Проект TERMES, реализуемый в течение четырех лет исследовательской группой самоорганизующихся систем Гарвардского университета, в основе которого лежит моде­лирование поведения колонии термитов, имеет конечную цель в создании масштабируемой системы искусственного интеллекта, в основе которой лежат простейшие роботы, способные уже сейчас совместными усилиями строить башни, пирамиды и другие сооружения, возводя даже до­полнительные элементы, позволяющие роботам подни­маться выше.

Данный проект имеет абсолютно другой подход к ор­ганизации работ, нежели традиционная иерархическая система, в которой основной план движется, дробясь на множество мелких задач, от руководителей высшего звена через череду менеджеров и специалистов к непосредствен­ным исполнителям. Вместо этого, модель колонии терми­тов предусматривает выполнение работ каждым роботом обособленно, без всякого централизованного руководства. Исследователи объясняют, что роботы действуют при по­мощи принципа стигмергии (stigmergy), принципа неяв­ных коммуникаций, когда каждый индивидуум распознает изменения окружающей его среды и корректирует свои собственные планы в соответствии с этими изменениями.

Благодаря использованию принципа стигмергии, ро­боты TERMES могут работать группами от нескольких эк­земпляров до нескольких тысяч, выполняя единую задачу, но абсолютно не общаясь друг с другом. Отсутствие цен­трализованного управления означает, что у системы в це­лом имеется крайне высокий уровень надежности, выход из строя одного экземпляра робота не приводит к неработо­способности системы, а оставшиеся работы продолжают работу, не замечая этого факта. Такой подход позволяет сделать роботов максимально простыми, ведь им не требу­ется наличия радио- или другого коммуникационного ка­нала, работающего на иных принципах. Роботы TERMES, созданные гарвардскими исследователями, имеют всего по четыре датчика, по три независимых привода и несложный механизм, позволяющий брать, переносить и укладывать строительные блоки.

**4. Give the summary of the text using the key terms.**

**ARTIFICIAL LIFE**

**Read the following words and word combinations and use them for understanding and translation of the text:**

**manifold** - разнообразный, многообразный

**blanket term** - общий термин

**design space** - пространство проектных решений (пара-метров)

**generalize** - обобщать

**to conceive** - задумать, замыслить, разработать

**typified** - на примере

**crossover** - кроссинговер (перекрест хромосом)

**to intervene** - вмешиваться

**full-blown design** - полнофункциональная модель (об-разец)

**laypeople** - непрофессионалы

**carbon chemistry** - химия углеродных соединений

**species of prey** - хищный вид

**predator** - хищник

**to validate** - подтверждать, проверять правильность

**conversely** - наоборот, напротив, с другой стороны

**to remedy** - лечить, исправлять

**commitment to the idea** - приверженность идее

**autopoiesis** - самосоздание, самовоспроизводство

The historical and theoretical roots of the field are manifold. These roots include:

* early attempts to imitate the behavior of humans and animals by the invention of mechanical automata in the sixteenth century;
* cybernetics as the study of general principles of informational control in machines and animals;
* computer science as theory and the idea of abstract equivalence between various ways to express the notion of computation, including physical instantiations of systems performing computations;
* John von Neumann's so-called self-reproducing Cellular Automata;
* computer science as a set of technical practices and computational architectures;
* artificial intelligence (AI)
* robotics;
* philosophy and system science notions of levels of organization, hierarchies, and emergence of new properties;
* non-linear science, such as the physics of complex systems and chaos theory; theoretical biology, including abstract theories of life processes; and
* evolutionary biology.

**Artificial life** is a blanket term used to refer to human attempts at setting up systems with lifelike properties all biological organisms possess, such as self-reproduction, homeostasis, adaptability, mutational variation, optimization of external states, and so on. The term is commonly associated with computer simulation-based artificial life, preferred heavily to robotics because of its ease of reprogramming, inexpensive hardware, and greater design space to explore. Artificial life projects can be thought of as attempts to generalize the phenomenon of life, asking questions like, "what would life have looked like if it evolved under radically different physical conditions?", "what is the logical form of all living systems?", or "what is the simplest possible living system?"

The term "artificial life", often shortened to "alife" or "A-Life", was coined in the late 1980s by researcher Christopher Langton, who defined it as "the study of artificial systems that exhibit behavior characteristic of natural living systems. It is the quest to explain life in any of its possible manifestations, without restriction to the particular examples that have evolved on earth... the ultimate goal is to extract the logical form of living systems."

Probably the first person to actively study and write on topics related to A-Life was the noted mathematician John Von Neumann, who was also an early figure in the field of game theory. In the middle of the 20th century, Von Neumann delivered a paper entitled "The General and Logical Theory of Automata," in which he discussed the concept of a machine that follows simple rules and reacts to information in its environment. Von Neumann proposed that living organisms are just such machines. He also studied the concept of machine self-replication, and conceived the idea that a self-replicating machine, or organism, must contain within itself a list of instructions for producing a copy of itself. This was several years before James Watson and Francis Crick, with the help of Rosalind Franklin and Maurice Wilkins, discovered the structure of DNA.

The field was expanded by the development of cellular automata as typified in John Conway’s Game of Life in the 1970s, which demonstrated how simple components interacting according to a few specific rules could generate complex emergent patterns. This principle is used to model the flocking behavior of simulated birds, called “boids”.

The development of genetic algorithms by John Holland added selection and evolution to the act of reproduction. This approach typically involves the setting up of numerous small programs with slightly varying code, and having them attempt a task such as sorting data or recognizing patterns. Those programs that prove most “fit” at accomplishing the task are allowed to survive and reproduce. In the act of reproduction, biological mechanisms such as genetic mutation and crossover are allowed to intervene. A rather similar approach is found in the neural network, where those nodes that succeed better at the task are given greater “weight” in creating a composite solution to the problem.

A more challenging but interesting approach to AL is to create actual robotic “organisms” that navigate in the physical rather than the virtual world. Roboticist Hans Moravec of the Stanford AI Laboratory and other researchers have built robots that can deal with unexpected obstacles by improvisation, much as people do, thanks to layers of software that process perceptions, fit them to a model of the world, and make plans based on goals. But such robots, built as full-blown designs, share few of the characteristics of artificial life. As with AI, the bottom-up approach offers a different strategy that has been called “fast, cheap, and out of control”—the production of numerous small, simple, insectlike robots that have only simple behaviors, but are potentially capable of interacting in surprising ways. If a meaningful genetic and reproductive mechanism can be included in such robots, the result would be much closer to true artificial life.

Artificial life is still a very new discipline, having been founded only in the late 1980s, and is still very much under development. Like other new fields, it has been the subject of some criticism. Based on its abstract nature, artificial life has taken time to be understood and accepted by the mainstream; papers on the topic have only recently been put into prominent scientific publications like *Nature* and *Science*. As with any new discipline, researchers need time to select the most fruitful research paths and translate their findings into terms other scientists and laypeople can understand and appreciate. The field of artificial life is one that seems poised to grow as the cost of computing power continues to drop.

Artificial life may be labeled **software**, **hardware**, or **wetware**, depending on the type of media researchers work with.

**Software artificial life** is rooted in computer science and represents the idea that life is characterized by form, or forms of organization, rather than by its constituent material. Thus, "life" may be realized in some form (or media) other than carbon chemistry, such as in a computer's central processing unit, or in a network of computers, or as computer viruses spreading through the Internet. One can build a virtual ecosystem and let small component programs represent species of prey and predator organisms competing or cooperating for resources like food.

The difference between this type of artificial life and ordinary scientific use of computer simulations is that, with the latter, the researcher attempts to create a model of a real biological system (e.g., fish populations of the Atlantic Ocean) and to base the description upon real data and established biological principles. The researcher tries to validate the model to make sure that it represents aspects of the real world. Conversely, an artificial life model represents biology in a more abstract sense; it is not a real system, but a virtual one, constructed for a specific purpose, such as investigating the efficiency of an evolutionary process of a Lamarckian type (based upon the inheritance of acquired characters) as opposed to Darwinian evolution (based upon natural selection among randomly produced variants). Such a biological system may not exist anywhere in the real universe. As Langton emphasized, artificial life investigates "the biology of the possible" to remedy one of the inadequacies of traditional biology, which is bound to investigate how life actually evolved on Earth, but cannot describe the borders between possible and impossible forms of biological processes. For example, an artificial life system might be used to determine whether it is only by historical accident that organisms on Earth have the universal genetic code that they have, or whether the code could have been different.

It has been much debated whether virtual life in computers is nothing but a model on a higher level of abstraction, or whether it is a form of genuine life, as some artificial life researchers maintain. In its computational version, this claim implies a form of Platonism whereby life is regarded as a radically medium-independent form of existence similar to futuristic scenarios of disembodied forms of cognition and AI that may be downloaded to robots. In this debate, classical philosophical issues about dualism, monism, materialism, and the nature of information are at stake, and there is no clear-cut demarcation between science, metaphysics, and issues of religion and ethics.

**Hardware artificial life** refers to small animal-like robots, usually called animats, that researchers build and use to study the design principles of autonomous systems or agents. The functionality of an agent (a collection of modules, each with its own domain of interaction or competence) is an emergent property of the intensive interaction of the system with its dynamic environment. The modules operate quasi-autonomously and are solely responsible for the sensing, modeling, computing or reasoning, and motor control that is necessary to achieve their specific competence. Direct coupling of perception to action is facilitated by the use of reasoning methods, which operate on representations that are close to the information of the sensors.

This approach states that to build a system that is intelligent it is necessary to have its representations grounded in the physical world. Representations do not need to be explicit and stable, but must be situated and "embodied." The robots are thus situated in a world; they do not deal with abstract descriptions, but with the environment that directly influences the behavior of the system. In addition, the robots have "bodies" and experience the world directly, so that their actions have an immediate feedback upon the robot's own sensations. Computer-simulated robots, on the other hand, may be "situated" in a virtual environment, but they are not embodied. Hardware artificial life has many industrial and military technological applications.

**Wetware artificial life** comes closest to real biology. The scientific approach involves conducting experiments with populations of real organic macromolecules (combined in a liquid medium) in order to study their emergent self-organizing properties. An example is the artificial evolution of ribonucleic acid molecules (RNA) with specific catalytic properties. (This research may be useful in a medical context or may help shed light on the origin of life on Earth.) Research into RNA and similar scientific programs, however, often take place in the areas of molecular biology, biochemistry and combinatorial chemistry, and other carbon-based chemistries. Such wetware research does not necessarily have a commitment to the idea, often assumed by researchers in software artificial life, that life is a composed of medium-in-dependent forms of existence.

Thus wetware artificial life is concerned with the study of self-organizing principles in "real chemistries." In theoretical biology, autopoiesis is a term for the specific kind of self-maintenance produced by networks of components producing their own components and the boundaries of the network in processes that resemble organizationally closed loops. Such systems have been created artificially by chemical components not known in living organisms.

The philosophical implications arising from the possible development of true artificial life are similar to those involved with “strong AI.” Human beings are used to viewing themselves as the pinnacle of a hierarchy of intelligence and creativity. However, artificial life with the capability of rapid evolution might quickly outstrip human capabilities, perhaps leading to a world like that portrayed by science fiction writers where flesh-and-blood humans become a marginalized remnant population.

**Notes:**

**Cellular Automaton** is a collection of "colored" cells on a grid of specified shape that evolves through a number of discrete time steps according to a set of rules based on the states of neighboring cells. The rules are then applied iteratively for as many time steps as desired.

**homeostasis** is the ability to maintain a constant internal environment in response to environmental changes.

**DNA** or deoxyribonucleic acid is the hereditary material in humans and almost all other organisms that encodes the genetic instructions used in the development and functioning of all known living [org](http:///h)a[nisms](http:///h) and many viruses.

**Game of Life,** also known simply as **Life**, is a cellular automaton devised by the [B](http:///h)r[itish](http:///h) mathematician John Horton Conway in 1970. The "game" is a zero-player game, meaning that its evolution is determined by its initial state, requiring no further input. One interacts with the Game of Life by creating an initial configuration and observing how it evolves.

**Hans Moravec** (born November 30, 1948, Kautzen, Austria) is an adjunct faculty member at the Robotics Institute of Carnegie Mellon University. He is known for his work on robotics, artificial intelligence, and writings on the impact of techno[logy](http:///h). Moravec also is a futurist with many of his publications and predictions focusing on transhumanism. Moravec developed techniques in computer vision for determining the region of interest (ROI) in a scene.

**animats** are artificial [an](http:///h)imals, a contraction of animal-materials. The term includes physical robots and virtual simulations.

**ribonucleic acid (RNA)** is a ubiquitous family of large biological molecules that perform multiple vital roles in the coding, decoding, regulation, and expression of [genes](http:///h). Together with DNA, RNA comprises the nucleic acids, which, along with proteins, constitute the three major macromolecules essential for all known forms of life.

**autopoiesis** (from Greek αὐτo- *(auto-)*, meaning "self", and ποίησις *(poiesis)*, meaning "creation, production") refers to a system capable of reproducing and maintaining itself.

**Assignments**

**1. Translate the sentences from the texts into Russian in writing paying attention to the underlined words and phrases:**

1. The term is commonly associated with computer simulation-based artificial life, preferred heavily to robotics because of its ease of reprogramming, inexpensive hardware, and greater design space to explore.
2. It is the quest to explain life in any of its possible manifestations, without restriction to the particular examples that have evolved on earth... the ultimate goal is to extract the logical form of living systems.
3. This principle is used to model the flocking behavior of simulated birds, called “boids”.
4. This approach typically involves the setting up of numerous small programs with slightly varying code, and having them attempt a task such as sorting data or recognizing patterns.
5. As Langton emphasized, artificial life investigates "the biology of the possible" to remedy one of the inadequacies of traditional biology, which is bound to investigate how life actually evolved on Earth, but cannot describe the borders between possible and impossible forms of biological processes.
6. The functionality of an agent (a collection of modules, each with its own domain of interaction or competence) is an emergent property of the intensive interaction of the system with its dynamic environment.
7. This approach states that to build a system that is intelligent it is necessary to have its representations grounded in the physical world.

**2. Answer the following questions:**

1. What are the origins of A-life as a discipline?
2. What questions are believed to be central to the field of A-life?
3. What does the concept of Cellular Automata involve?
4. Which of the three types of A-life seems to be most promising?
5. What are the distinguishing features of each type?
6. What kind of ethic issues might arise concerning A-life?

**3. Translate into English:**

**Искусственная жизнь создана! Возможно ли такое?**

24 мая 2010 года на пресс-конференции известный и талантливый американский биолог и бизнесмен Вентер, первый в мире расшифровавший геном человека, объявил общественности, что под его руководством институтом его же имени создана искусственная жизнь.

Впервые в истории создана искусственная живая клетка, которая всецело управляется рукотворным гено­мом.Ранее ученые лишь редактировали ДНК по кусочкам, получая генномодифицированные растения и животных.

Это достижение, несомненно, подогреет споры об этичности создания искусственной жизни, а также о юри­дически-правовых моментах и общественной опасности таких работ. "Это поворотный момент в отношениях чело­века с природой: впервые создана целая искусственная клетка с заранее заданными свойствами", - пояснил моле­кулярный биолог Ричард Эбрайт из Университета Рутд­жерса. По мнению экспертов, вскоре метод будет использо­ваться в коммерческих целях: некоторые компании уже разрабатывают живые организмы, способные синтезиро­вать топливо, вакцины и др. Компания Synthetic Genomics Inc., основанная Вентером, заключила контракт на 600 млн. долларов на разработку водорослей, способных поглощать углекислый газ и производить топливо.

Ученые фактически претворили компьютерную про­грамму в новое живое существо. Взяв за основу одну из бак­терий, они внесли в компьютер полную расшифровку ее генома, заменили некоторые фрагменты в этом "тексте" своими собственными "сочинениями" и получили моди­фицированный вариант бактерии другого реально сущест­вующего вида. "Мы изготавливаем геном из четырех пу­зырьков химикатов, вносим искусственный геном в клетку, и наш искусственный геном подчиняет клетку себе", - разъ­яснил один из руководителей проекта Дэниел Гибсон. Чтобы обособить эту новую бактерию и всех ее потомков от творений природы, Вентер и его коллеги вставили в геном свои имена, а также три цитаты из Джеймса Джойса и дру­гих авторов. Эти "генетические водяные знаки" помогут ученым предъявить право собственности на клетки.

**Topics for essays (you might need additional information):**

* Early automatons
* Famous robotics projects
* Swarm intelligence: pros and cons
* Chemically Synthesized Genome

**FUTURE COMPUTING**

**QUANTUM COMPUTING**

**Read the following words and word combinations and use them for understanding and translation of the text:**

**property** - свойство, качество

**quantum** - квант. квантовый

**spin** - вращение

**superposition** - суперпозиция, наложение, совмещение

**to flesh out** - конкретизировать, изложить в деталях

**to spur** - побуждать, стимулировать

**in part** - частично

**to outline** - намечать, изложить вкратце

**to factor** - факторизовать, разложить (на множители)

**integer** - целое число

**to be of great interest (to)** - представлять большой интерес (для)

**to tackle** - заниматься

**entanglement** - перепутывание (квантовых состояний)

**to crack** - раскалывать(ся), ломаться

**civilian** - гражданский

The fundamental basis of electronic digital computing is the ability to store a binary value (1 or 0) using an electromagnetic property such as electrical charge or magnetic field.

However, during the first part of the 20th century, physicists discovered the laws of quantum mechanics that apply to the behavior of subatomic particles. An electron or photon, for example, can be said to be in any one of several “quantum states” depending on such characteristics as spin. In 1981, physicist Richard Feynman came up with the provocative idea that if quantum properties could be “read” and set, a computer could use an electron, photon, or other particle to store not just a single 1 or 0, but a number of values simultaneously. This ability of a quantum system to be in multiple states at the same time is called *superposition*. The simplest case, storing two values at once, is called a “qubit” (short for “quantum bit”). In 1985, David Deutsch at Oxford University fleshed out Feynman’s ideas by creating an actual design for a “quantum computer”, including an algorithm to be run on it.

At the time of Feynman’s proposal, the techniques for manipulating individual atoms or even particles had not yet been developed, so a practical quantum computer could not be built. However, during the 1990s, considerable progress was made, spurred in part by the suggestion of Bell Labs researcher Peter Shor, who outlined a quantum algorithm that might be used for rapid factoring of extremely large integers. Since the security of modern public key cryptography depends on the difficulty of such factoring, a working quantum computer would be of great interest to spy agencies.

The reason for the tremendous potential power of quantum computing is that if each qubit can store two values simultaneously, a register with three qubits can store eight values, and in general, for *n* qubits one can operate on 2*n* values simultaneously. This means that a single quantum processor might be the equivalent of a huge number of separate processors. Clearly many problems that have been considered not practical to solve might be tackled with quantum computers.

Quantum computers also utilize another aspect of quantum mechanics known as *entanglement.* Unfortunately, quantum particles cannot be observed without being altered. Scientists use their knowledge of entanglement to indirectly observe the value of a qubit. When two subatomic particles become entangled, one particle adopts the properties of the other. Without looking at the qubit itself, scientists can read its value by observing the behavior of a particle with which it is entangled.

There are many potential applications for quantum computing. While the technology could be used to crack conventional cryptographic keys, researchers have suggested that it could also be used to generate unbreakable keys that depend on the “entanglement” of observers and what they observe. The sheer computational power of a quantum computer might make it possible to develop much better computer models of complex phenomena such as weather, climate, and the economy – or of quantum behavior itself.

As of 2014 quantum computing is still in its infancy but experiments have been carried out in which quantum computational operations were executed on a very small number of qubits. Both practical and theoretical research continues, and many national governments and military funding agencies support quantum computing research to develop quantum computers for both civilian and national security purposes, such as cryptanalysis.

**Notes:**

**Bell Labs (Bell Laboratories)** - бывшая американская, а ныне франко-американская корпорация, крупный исследова­тельский центр в области телекоммуникаций, электронных и компьютерных систем. Штаб-квартира Bell Labs располо­жена в Мюррей Хилл (Нью-Джерси, США)

**Assignments**

**1. Translate the sentences from the text into Russian in writing paying attention to the underlined words and phrases:**

1. However, during the 1990s, considerable progress was made, spurred in part by the suggestion of Bell Labs researcher Peter Shor, who outlined a quantum algorithm that might be used for rapid factoring of extremely large integers.
2. Since the security of modern public key cryptography depends on the difficulty of such factoring, a working quantum computer would be of great interest to spy agencies.
3. Unfortunately, quantum particles cannot be observed without being altered.
4. As of 2014 quantum computing is still in its infancy but experiments have been carried out in which quantum computational operations were executed on a very small number of qubits.
5. Both practical and theoretical research continues.

**2. Answer the following questions:**

1. What is the basis of electronic digital computing?
2. What provocative idea did physicist Richard Feynman come up with?
3. Why could a practical quantum computer not be built at the time of Feynman’s proposal?
4. Describe the reason for a huge potential power of quantum computing.
5. What aspects of quantum mechanics do quantum computers utilize?
6. How can quantum computing be applied?

**3. Translate into English:**

Современные компьютерные чипы могут содержать до нескольких миллиардов транзисторов на одном квадрат­ном сантиметре кремния, а в будущем подобные элементы не будут превышать размера молекулы. Устройства с та­кими чипами будут существенно отличаться от классиче­ских компьютеров. Это обусловлено тем, что принципы их работы будут основаны на квантовой механике, физиче­ских законах, объясняющих поведение атомов и субатом­ных частиц. Ученые надеются, что квантовые компьютеры смогут решать ряд специфических задач гораздо быстрее, чем их классические собратья.

В действительности создать квантовый компьютер не­просто. Основные его элементы - атомы, фотоны или спе­циально созданные микроструктуры, хранящие данные в так называемых кубитах (квантовых битах), особенность которых заключается в том, что они должны отвечать двум противоречивым требованиям. С одной стороны они должны быть достаточно изолированы от любых внешних воздействий, которые могут нарушить вычислительный процесс, а с другой - иметь возможность взаимодействовать с другими кубитами. Кроме того необходимо иметь воз­можность измерить окончательное состояние кубитов и отобразить результаты вычислений.

Ученые во всем мире используют несколько подходов для создания первых прототипов квантовых компьютеров.

**4. Give the summary of the text using the key terms.**

**BIOINFORMATICS**

**Read the following words and word combinations and use them for understanding and translation of the text:**

**undertaking** - предприятие, начинание, дело

**inherently** - по существу

**gene** - ген

**intricate** - сложный, запутанный

**protein folding** - сворачивание белков

**unlikely** - невероятный, малообещающий

**to harness** - использовать

**simulation** - моделирование

**makeup** - состав, структура, строение

**advent** - приход, появление

**predator** - хищник

**to devise** - разрабатывать, придумывать, изобретать

**sophisticated** - сложный

**feasible** - возможный, осуществимый

**to probe** - исследовать, прозондировать

**to bridge the gap** - устранить разрыв

**emergent behavior** - непредсказуемое поведение

**to inspire** - вдохновлять, воодушевлять

Broadly speaking, bioinformatics (and the related field of computational biology) is the application of mathematical and information-science techniques to biology. This undertaking is inherently difficult because a living organism represents such a complex interaction of chemical processes. As more has been learned about the genome of humans and other organisms, it has become increasingly clear that the ”programs” represented by gene sequences are “interpreted” through complex interactions of genes and the environment. Given this complexity, the great strides that have been made in genetics and the detailed study of metabolic and other biological processes would have been impossible without advances in computing and computer science.

**Application to genetics.**

Since information in the form of DNA sequences is the heart of genetics, information science plays a key role in understanding its significance and expression. The sequences of genes that determine the makeup and behavior of organisms can be represented and manipulated as strings of symbols using, for example, indexing and search algorithms. It is thus natural that the advent of powerful computer workstations and automated lab equipment would lead to the automation of gene sequencing, comparing or determining the relationship between corresponding sequences. The completion of the sequencing of the human genome well ahead of schedule was thus a triumph of computer science as well as biology.

**From genes to protein.**

Gene sequences are only half of many problems in biology. Computational techniques are also being increasingly applied to the analysis and simulation of the many intricate chemical steps that link genetic information to expression in the form of particular protein and its three-dimensional structure in the process known as protein folding. The development of better algorithms and more powerful computing architectures for such analysis can further speed up research, avoid wasteful “dead ends”, and bring effective treatments for cancer and other serious diseases to market sooner. The unlikely platform of a Sony PlayStation 3 and its powerful processor has been harnessed to turn gamers’ idle time to the processing of protein-folding data in the Folding@Home project.

**Simulation**

A variety of other types of biological computer simulation have been employed. Examples include the chemical components that are responsible for metabolic activity in organisms, the structure of the nervous system and the brain (neural network), and the interaction of multiple predators and food sources in an ecosystem. Simulations can also incorporate algorithms first devised by artificial intelligence researchers (genetic algorithms). Simulations are combined with sophisticated graphics to enable researchers to visualize structure. Visualization algorithms developed for biomedical research can also be applied to the development of advanced MRI and other scans for use in diagnosis and therapy.

**A fruitful relationship**

Bioinformatics has been one of the ”hottest” areas in computing in recent years, often following trends in the broader “biotech” sector. This challenging field involves such diverse subjects as genetics, biochemistry, physiology, mathematics (structural and statistical), database analysis and search techniques, simulation, modeling, graphics and image analysis. Major projects often involve close cooperation between bioinformatics specialists and other researchers. Researchers must also consider how the availability of ever-increasing computing power might make previously impossible projects feasible.

The relationship between biology and computer science seems destined to be even more fruitful in coming years. As software tools allow researchers to probe ever more deeply into biological processes and to bridge the gap between physics, biochemistry, and the emergent behavior of the living organisms, understanding of those processes may in turn inspire the creation of new architectures and algorithms in areas such as artificial intelligence and robotics.

**Notes:**

**DNA (Deoxyribonucleic acid)** - дезоксирибонуклеиновая кислота (ДНК)- макромолекула, обеспечивающая хранение, передачу из поколения в поколение и реализацию генетической программы развития и функционирования живых организмов.

**Folding@Home** - проект распределенных вычислений для проведения компьютерного моделирования свертывания молекул белка

**MRI (Magnetic Resonance Imaging)** – магнитно-резонансная томография

**Assignments**

**1. Translate the sentences from the text into Russian in writing paying attention to the underlined words and phrases.**

1. Broadly speaking, bioinformatics (and the related field of computational biology) is the application of mathematical and information-science techniques to biology.
2. Given this complexity, the great strides that have been made in genetics and the detailed study of metabolic and other biological processes would have been impossible without advances in computing and computer science.
3. The completion of the sequencing of the human genome well ahead of schedule was thus a triumph of computer science as well as biology.
4. Understanding of those processes may in turn inspire the creation of new architectures and algorithms in areas such as artificial intelligence and robotics.
5. The relationship between biology and computer science seems destined to be even more fruitful in coming years.

**2. Answer the following questions:**

1. What is bioinformatics?
2. How did advances in computing and computer science affect the development of genetics?
3. Why is information science so important for understanding genetics?
4. Describe the applications of computational techniques in the research of genetics.
5. How is the relationship between biology and computer science supposed to develop in future?

**3. Translate into English:**

В настоящее время, когда каждый новый шаг в совер­шенствовании полупроводниковых технологий дается со все большим трудом, ученые ищут альтернативные воз­можности развития вычислительных систем. Естественный интерес ряда исследовательских групп вызвали природные способы хранения и обработки информации в биологиче­ских системах. Итогом их изысканий явился гибрид ин­формационных и молекулярных технологий и биохимии - биокомпьютер.

Потенциал биокомпьютеров очень велик. По сравне­нию с обычными вычислительными устройствами они имеют ряд уникальных особенностей. Во-первых, они ис­пользуют не бинарный, а тернарный код (так как инфор­мация в них кодируется тройками нуклеотидов). Во-вто­рых, поскольку вычисления производятся путем одновре­менного вступления в реакцию триллионов молекул ДНК, они могут выполнять до 1014 операций в секунду. В-третьих, вычислительные устройства на основе хранят данные с плотностью, в триллионы раз превышающей по­казатели оптических дисков. И наконец, ДНК-компьютеры имеют исключительно низкое энергопотребление.

Другим перспективным направлением замены полу­проводниковых компьютеров является создание клеточных (бактериальных) компьютеров. Они представляют собой самоорганизующиеся колонии различных «умных» микро­организмов. С помощью клеточных компьютеров станет возможным непосредственное объединение информаци­онной технологии и биотехнологии.

Биокомпьютеры не рассчитаны на широкие массы пользователей. Но ученые надеются, что они найдут свое место в медицине и фармации. Глава израильской исследо­вательской группы профессор Эхуд Шапиро уверен, что в перспективе ДНК-наномашины смогут взаимодействовать с клетками человека, осуществлять наблюдение за потенци­альными болезнетворными изменениями и синтезировать лекар­ства для борьбы с ними.

**4. Give the summary of the text using the key terms.**

**NANOTECHNOLOGY**

**Read the following words and word combinations and use them for understanding and translation of the text:**

**to space** - расставлять

**precisely** - точно, в точности

**implication** - значение, роль

**density** - плотность

**to dissipate** - рассеивать

**to overcome** - преодолевать

**dormant** - дремлющий, находящийся в состоянии покоя

**branch** - ответвление

**assembly** - сборка, монтаж

**replication** – копирование, репродукция

**to deposit** – поместить, помещать

**nanotube** - нанотрубка

**conductor** - проводник

**to shrink** - сокращаться

**counterpart** - двойник, аналог

**core** - ядро, сердечник, стержень

**ultimate** - конечный, окончательный

In a talk given in 1959, physicist Richard Feynman suggested that it might be possible to manipulate atoms individually, spacing them precisely. As Feynman also pointed out, the implications of computer technology are potentially very impressive. A current commercial DIMM memory module about the size of a person’s little finger holds about 250 megabytes worth of data. Feynman calculated that if 100 precisely arranged atoms were used for each bit of information, the contents of all the books that have ever been written could be stored in a cube about 1/200 of an inch wide, just about the smallest object the unaided human eye can see. Further, although the density of computer logic circuits in microprocessors is millions of times greater than it was with the computers of 1959, computers built at the atomic scale would be billions of times smaller still. Indeed, they would be the smallest computers possible short of one that used quantum states within the atoms themselves to store information. “Nanocomputers” could also efficiently dissipate heat energy, overcoming a key problem with today’s increasingly dense microprocessors.

The idea of atomic-level engineering lay largely dormant for about two decades. Starting with a 1981 paper, however, K. Eric Drexler began to flesh out proposed structures and methods for a branch of engineering he termed *nanotechnology.* (The “nano” refers to a nanometer, or one billionth of a meter. The term “nanotechnology had been coined by the Tokyo Science University Professor Norio Taniguchi in 1974, and Drexler unknowingly used a related term to describe what later became known as molecular nanotechnology). Research in nanotechnology focuses on two broad areas: assembly and replication. Assembly is the problem of building tools (called assemblers) that can deposit and position individual atoms. Since such tools would almost certainly be prohibitively expensive to manufacture individually, research has focused on the idea of making tools that can reproduce themselves. This area of research began with John von Neumann’s 1940s concept of self-replicating computers.

There are several potential applications of nanotechnology in the manufacture of computer components. One is the possible use of carbon nanotubes in place of copper wires as conductors in computer chips. As chips continue to shrink, the connectors have also had to get smaller, but this in turn increases electrical resistance and reduces efficiency. Nanotubes, however, are not only superb electrical conductors, they are also far thinner than their copper counterparts. Intel Corporation has conducted promising tests of nanotube conductors, but it will likely be a number of years before they can be manufactured on an industrial scale.

Another alternative is “nanowires”. One design consists of a germanium core surrounded by a thin layer of crystalline silicon. Nanowires are easier to manufacture than nanotubes, but their performance and other characteristics may make them less useful for general-purpose computing devices.

The ultimate goal is to make the actual transistors in computer chips out of nanotubes instead of silicon. An important step in this direction was achieved in 2006 by IBM researchers who created a complete electronic circuit using a single carbon nanotube molecule.

**Notes:**

**DIMM (Dual In-line Memory Module)** - двусторонний модуль памяти

Intel Corporation - американская корпорация, производящая широкий спектр электронных устройств и компьютерных компонентов, включая микропроцессоры, наборы системной логики (чипсеты) и др. Штаб-квартира - в городе Санта-Клара (Калифорния, США).

**Assignments**

**1. Translate the sentences from the text into Russian in writing paying attention to the underlined words and phrases:**

1. A current commercial DIMM memory module about the size of a person’s little finger holds about 250 megabytes worth of data.
2. Indeed, they would be the smallest computers possible short of one that used quantum states within the atoms themselves to store information.
3. The idea of atomic-level engineering lay largely dormant for about two decades.
4. Starting with a 1981 paper, however, K. Eric Drexler began to flesh out proposed structures and methods for a branch of engineering he termed *nanotechnology.*
5. One is the possible use of carbon nanotubes in place of copper wires as conductors in computer chips.
6. Intel Corporation has conducted promising tests of nanotube conductors, but it will likely be a number of years before they can be manufactured on an industrial scale.

**2. Answer the following questions:**

1. When was the idea to manipulate atoms individually first suggested?
2. What is nanotechnology?
3. Research in nanotechnology focuses on two broad areas. What are they?
4. Describe the potential applications of nanotechnology in manufacturing computer components.
5. What is the ultimate goal of nanotechnology in the field of manufacturing computers?

**3. Translate into English:**

В 1959 году Ричард Фейнман в своем выступлении предсказал, что в будущем, научившись манипулировать отдельными атомами, человечество сможет синтезировать все, что угодно. В 1981 году появился первый инструмент для манипуляции атомами - туннельный микроскоп, изо­бретенный учеными из IBM. Оказалось, что с помощью этого микроскопа можно не только «видеть» отдельные атомы, но и поднимать и перемещать их. Этим была про­демонстрирована принципиальная возможность манипу­лировать атомами, а стало быть, непосредственно собирать из них, словно из кирпичиков, все, что угодно: любой предмет, любое вещество.

Нанотехнологии обычно делят на три направления:

- изготовление электронных схем, элементы которых состоят из нескольких атомов

- создание наномашин, т.е. механизмов и роботов раз­мером с молекулу

- непосредственная манипуляция атомами и молеку­лами.

Благодаря стремительному прогрессу в таких техноло­гиях, как оптика, нанолитография, механохимия и 3D про­тотипирование, нанореволюция может произойти уже в течение следующего десятилетия. Когда это случится, на­нотехнологии окажут влияние практически на все области промышленности и общества.

**4. Give the summary of the text using the key terms.**

**UBIQUITOUS COMPUTING**

**Read the following words and word combinations and use them for understanding and translation of the text:**

**discrete** - дискретный

**ubiquitous** - повсеместный, вездесущий

**pervasive** - распространенный, всеобъемлющий

**to communicate** - сообщать, передавать

**to tag** - добавлять

**to track** - прослеживать

**to predict** - прогнозировать

**tiny** - крошечный

**to embed** - встраивать

**to run out** - кончаться, истощаться

**ambient** - окружающий

**to attune (to)** – настраивать (на)

**dashboard** - информационная панель

**cue** - сигнал, намек

**seamlessly** - легко, беспрепятственно, без проблем

**wearable** - носимый

Traditionally people have thought of computers as discrete devices used for specific purposes such as to send e-mail or browse the Web. However, many researchers and futurists are looking toward a new paradigm that is rapidly emerging. Ubiquitous (or pervasive) computing focuses not on individual computers and tasks but on a world where most objects (including furniture and appliances) have the ability to communicate information. Kevin Ashton, a British technologist who created a system for tagging and tracking objects using radio frequencies, has predicted a future where everything is connected to the internet via tiny computer chips embedded within, or as he called it “the Internet of things”. A fridge is already available with an on-board computer, allowing it to know its contents, order food when you run out and even suggest suitable recipes, before setting the oven to the right cooking temperature. It is also currently possible to control an entire room- the thermostat, light switch, TV, stereo etc.- all from a tablet or smartphone using wirelessly connected chips in each of the controlled devices.

“The internet of things” can be viewed as the third phase in a process where the emphasis has gradually shifted from individual desktops (1980s) to the network and Internet (1990s) to mobile presence and the ambient environment.

Some examples of ubiquitous computing might include:

- picture frames that display pictures attuned to the user’s activities

- “dashboard” devices that can be set to display changing information such as weather and stock quotes

- parking meters that can provide verbal directions to nearby attractions

- kiosks or other facilities to provide verbal cues to guide travelers, such as through airports

- home monitoring systems that can sense and deal with accidents or health emergencies.

Ubiquitous computing greatly increases the ability of people to seamlessly access information for their daily activities. But the fact that the user is in effect “embedded” in the network can also raise issues of privacy and the receiving of unwanted advertising or other information.

An early center of research in ubiquitous computing was Xerox PARC, famous for its development of graphical user interface. Today a major force is MIT, especially its Project Oxygen, which explores networks of embedded computers. This challenging research area brings together aspects of many other fields (artificial intelligence, distributed computing, psychology of computing, smart buildings and homes, touchscreen, user interface, and wearable computers).

**Notes:**

**XeroxPARC (Xerox Palo Alto Research Center)** - научно-исследовательский центр, основанный в 1970. В 2002 году PARC стал отдельной компанией (в собственности Xerox)

**MIT** - Massachusetts Institute of Technology

**Project Oxygen**- исследовательский проект MIT для разработки вездесущих вычислений

**Assignments**

**1. Translate the sentences from the text into Russian in writing paying attention to the underlined words and phrases:**

1. “The internet of things” can be viewed as the third phase in a process where the emphasis has gradually shifted from individual desktops (1980s) to the network and Internet (1990s) to mobile presence and the ambient environment.
2. But the fact that the user is in effect “embedded” in the network can also raise issues of privacy.

**2. Answer the following questions:**

1. What is ubiquitous computing?
2. A British technologist K. Ashton has predicted “the Internet of things”. What does this mean?
3. Give examples of ubiquitous computing.
4. What are “the two sides of the coin” when using ubiquitous computing in daily life?
5. Who deals with the research in ubiquitous computing?

**3. Translate into English:**

Интернет вещей (The Internet of Things, IoT) - концеп­ция вычислительной сети физических объектов («вещей»), оснащенных встроенными технологиями для взаимодейст­вия друг с другом или с внешней средой. Организация та­ких сетей способно перестроить экономические и общест­венные процессы, исключая из части действий и операций необходимость участия человека.

Идея Интернета вещей сама по себе очень проста. Представим, что все окружающие нас предметы и устрой­ства (домашние приборы, одежда, продукты, автомобили, промышленное оборудование и др.) снабжены миниатюр­ными идентификационными и сенсорными устройствами. Тогда при наличии необходимых каналов связи с ними можно не только отслеживать эти объекты и их параметры в пространстве и во времени, но и управлять ими, а также включать информацию о них в общую «умную планету».

Концепция сформулирована в 1999году как осмысле­ние перспектив широкого применения средств радиочас­тотной идентификации для взаимодействия физических объектов между собой и с внешним окружением. Внедре­ние практических решений для ее реализации начиная с 2010 года считается восходящим трендом в информацион­ных технологиях, прежде всего, благодаря повсеместному распространению беспроводных сетей, появлению облач­ных вычислений, развитию технологии межмашинного взаимодействия и др.

**4. Give the summary of the text using the key terms.**

**SUPERCOMPUTERS**

**Read the following words and word combinations and use them for understanding and translation of the text:**

**successive** - последующий, преемственный

**at a clock speed** - с тактовой частотой

**to take advantage of** - воспользоваться

**entire** - целый, полный

**the ultimate** - в конечном итоге

**formerly** - раньше

**to soak up** - впитывать, поглощать

**protein** - белок

**cost-effective** - рентабельный

**distributed** - распределенный

**to feature** - показывать, изображать

**synergistic processing element** - ядро специального назначения

**ad hoc**- специальный, на данный случай

**to parcel out** - выделять, делить на части

**extraterrestrial** - внеземной

**proximity** - близость

**mesh** - сетка, ячейка

**to rank** - классифицировать

**high-performance computing** - высокопроизводительные вычисления

**benchmark** - отметка, стандарт, эталонный тест

**to retain** - сохранять. удерживать

The term *supercomputer* is not really an absolute term describing a unique type of computer. Rather it has been used through successive generations of computer design to describe the fastest, most powerful computers available at a given time. However, what makes these machines the fastest is usually their adoption of a new technology or computer architecture that later finds its way into standard computers.

The first supercomputer is generally considered to be the Control Data CDC 6600, designed by Seymour Cray in 1964. The speed of this machine came from its use of the new faster silicon (rather than germanium) transistors and its ability to run at a clock speed of 10 MHz (a speed that would be achieved by personal computers by the middle 1980s).

Cray then left CDC to form Cray Research. He designed *the Cray I* in 1976, the first of a highly successful series of supercomputers. The Cray I took advantage of a new technology: integrated circuits, and new architecture: vector processing, in which a single instruction can be applied to an entire series of numbers simultaneously. This innovation marked the use of parallel processing as one of the distinguishing features of supercomputers.

The next generation, the Cray X-MP carried parallelism further by incorporating multiple processors ( the successor, Cray Y-MP, had 8 processors which together could perform a billion floating point operations per second (1 gigaflop).

Soon other companies (particularly the Japanese manufactures NEC and Fujitsu) entered the market. The number of processors in supercomputers increased to as many as 1,024, which can exceed 1 trillion floating-point operations per second (1 teraflop)

The ultimate in multiprocessing is the series of Connection Machines built by Thinking Machines Inc. (TMI) and designed by Daniel Hillis. These machines have up to 65,000 very simple processors that run simultaneously and can form connections dynamically, somewhat like the process in the human brain. These “massively parallel” machines are thus attractive for artificial intelligence research.

As the power of standard computers continuous to grow, applications that formerly required a multimillion-dollar supercomputer can now run on a desktop workstation.

On the other hand there are always applications that will soak up whatever computing power can be brought to bear on them. These include: analysis of new aircraft designs, weather and climate models, the study of nuclear reactions, and the creation of models for the synthesis of proteins.

For many applications it may be more cost-effective to build systems with numerous coordinated processors (a sort of successor to the 1980s Connection Machine). For example, the Beowolf architecture involves “clusters” of ordinary PCs coordinated by software running on UNIX or Linux. The use of free software and commodity PCs can make this approach attractive, though application software still has to be rewritten to run on the distributed processors.

A new resource for parallel supercomputing came from an unlikely place: the new generation of cell processors found in game consoles such as the Sony Playstation 3. This architecture features tight integration of a central “power processor element” with multiple “synergistic processing elements”.

Finally, an ad hoc “supercomputer” can be created almost for free, using software that parcels out calculation tasks to thousands of computers participating via the Internet, as with SETI@Home (searching for extraterrestrial radio signals) and Folding@Home (for protein-folding analysis). In another approach, a large number of dedicated processors are placed in close proximity to each other (e.g. in a computer cluster); this saves considerable time moving data around and makes it possible for the processors to work together (rather than on separate tasks), for example in mesh and hypercube architecture.

The Top500 project ranks and details the 500 most powerful (non-distributed) computer systems in the world. The project was started in 1993 and publishes an updated list of the supercomputers twice a year. The project aims to provide a reliable basis for tracking and detecting trends in high-performance computing and bases rankings on HPL, a portable implementation of the high-performance LINPACK benchmark written in FORTRAN for distributed memory computers.

According to the 42nd edition (November, 2013) of the Top500 list of the world’s most powerful supercomputers, Teanhe-2, a supercomputer developed by China’s National University of Defense Technology, retained its position as the world’s No.1 system with a performance of 33.86 petaflops/s (quadrillions of calculations per second).

Titan, a Cray XK7 system installed at the Department of Energy’s (DOE) Oak Ridge National Laboratory, remains the No.2 system. It achieved 17.59 Pflops/s on the Linpack benchmark. Titan is one of the most energy-efficient systems on the list.

**Notes:**

**NEC (Nippon Electric Corporation)** - японская компания, производитель электронной, компьютерной техники

**Fujitsu** - крупная японская корпорация, производитель электроники

**SETI@Home** (Search for Extra-Terrestrial Intelligence at Home – поиск внеземного разума на дому) – научный некоммер­ческий проект добровольных вычислений на платформе BOINC, использующий свободные вычислительные ре­сурсы на компьютерах добровольцев для поиска радиосиг­налов внеземных цивилизаций

**LINPACK** benchmark - тест производительности вычисли­тельных систем, по результатам которого составляется спи­сок 500 наиболее высокопроизводительных систем мира

**Assignments**

**1. Translate the sentences from the text into Russian in writing paying attention to the underlined words and phrases:**

1. Rather it has been used through successive generations of computer design to describe the fastest, most powerful computers available at a given time.
2. The Cray I took advantage of a new technology: integrated circuits, and new architecture: vector processing, in which a single instruction can be applied to an entire series of numbers simultaneously.
3. The next generation, the Cray X-MP carried parallelism further by incorporating multiple processors.
4. On the other hand there are always applications that will soak up whatever computing power can be brought to bear on them.
5. Finally, an ad hoc “supercomputer” can be created almost for free, using software that parcels out calculation tasks to thousands of computers participating via the Internet.

**2. Answer the following questions:**

1. What does the term *supercomputer* describe?
2. What is considered to be the first supercomputer?
3. Which innovation marked the use of parallel processing as one of the distinguishing features of supercomputers?
4. Describe resources for parallel “supercomputing”.
5. What is Top500 project?

**3. Translate into English:**

**«Элита компьютерного мира»**

Суперкомпьютеры находятся на вершине своеобразной пирамиды мира вычислительной техники. Современные машины могут иметь до 100 тысяч процессоров и выпол­нять 60 000 млрд. операций в секунду. История суперком­пьютеров в СССР началась именно в МГУ. Первая машина «Стрела» была построена в 1956 году легендарным конст­руктором и основателем советской школы конструкторов вычислительной техники С.А. Лебедевым. «Стрела» вы­полняла 2000 операций в секунду и занимала 300 кв. м.

Следующая машина «БЭСМ-6», построенная в 1968 году, уже выполняла 1 млн. операций в секунду и являлась на тот момент одной из самых быстродействующих машин в мире.

В 2008 г. На базе НИВЦ МГУ был построен современ­ный суперкомпьютер «Чебышев», названный в честь вели­кого русского математика. Он занимает всего 100 кв. м., ве­сит 30 тонн и способен выполнять уже тысячи миллиардов операций в секунду.

Суперкомпьютер «Ломоносов», построенный компа­нией «Т-Платформы» для МГУ им. М.В. Ломоносова,- пер­вый гибридный суперкомпьютер такого масштаба в России и Восточной Европе. В нем используется три вида вычисли­тельных узлов и процессоры с различной архитектурой. Предполагается использовать суперкомпьютер для реше­ния ресурсоемких вычислительных задач в рамках фунда­ментальных научных исследований, а также для проведе­ния научной работы в области разработки алгоритмов и программного обеспечения для мощных вычислительных систем.

Суперкомпьютеры решают огромное количество важ­ных прикладных и фундаментальных задач. Одни из наи­более часто встречающихся - моделирование нефтяных ре­зервуаров, проектирование жилищных застроек и новых материалов, проведение виртуальных краш-тестов в про­цессе конструирования автомобилей. В МГУ «Чебышев» занимается фундаментальной наукой. На нем, в частности, решается задача исследования магнитного поля Земли. Не­заменимы суперкомпьютеры и в криптографии- науке о защите информации. Суперкомпьютер эффективно вы­полняет параллельные вычисления благодаря большому количеству самостоятельных микропроцессоров.

Не каждую задачу можно решить на суперкомпьютере: сложность задачи должна соответствовать сложности сис­темы. Самым большим суперкомпьютером, как это ни странно, является сеть Интернет, которая соединяет огром­ное количество вычислительных мощностей по всему миру. В будущем, возможно, удастся скоординировать усилия и использовать невостребованные мощности такой суперсис­темы.

**Topics for essays (you might need additional information):**

* Quantum computers versus traditional computers.
* Nanotechnology in our lives.
* The Internet of things may bring problems.
* Tiny biocomputers move closer to reality.
* Application of supercomputers.

**LITERATURE**

1. “3D Computer Graphics” by [Alan H. Watt](http://www.google.ru/search?hl=ru&tbo=p&tbm=bks&q=inauthor:%22Alan+H.+Watt%22), Addison-Wesley, 2000
2. “A Brief History of Programming Languages.”  [http://www.byte.com/art/9509/se7/artl9.htm](http:///h). Cited, March 25, 2000.
3. “Artificial Intelligence - What You Really Need to Know” by Michele Goetz. Jan 30, 2014 http://www.forbes.com/sites/forrester/2014/01/29/artificial-intelligence-what-you-really-need-to-know/
4. “Artificial Life. Encyclopedia of Science and Religion” by Claus Emmeche, New York University Press, 2003. http://www.encyclopedia.com/topic/Artificial\_life.aspx
5. “Best-Kept Secrets: Quantum Cryptography Has Marched from Theory to Laboratory to Real Products” by Stix, Gary. Scientific American, 2005. http://www.sciam.com/article.cfm?chanID=sa006&colID=1&articleID= 000479CD-F58C-11BE-AD0683414B7F0000
6. “Biometric Security Technology” by P Kumbargoudar, PeterIndia , 2008 www.peterindia.net/BiometricsView.html
7. “Cognitive Computing Ushers In New Era of IT” by Eric W. Brown, IBM Smarter Planet. 2/03/2014. http://www.forbes.com/sites/ibm/2014/02/03/cognitive-computing-ushers-in-new-era-of-it/
8. “Computer Graphics: Principles and Practice” by James D. Foley, Andries van Dam, Steven K. Feiner and John F. Hughes. Addison-Wesley Professional, 1996.
9. “Computer Graphics: Theory into Practice” by Jeffrey J. McConnell. Jones and Bartlett Publishers, 2006.
10. “Computer Science Illuminated” by Nell Dale, John Lewis. Jones and Bartlett Publishers, 2002
11. “Concepts and Terminology for Computer Security” by Donald L. Brinkley and Roger R. Schell, 1995
12. “Concepts in Programming Languages” by John C. Mitchell. Cambridge University Press, 2003
13. “Encyclopedia of Computer Science and Technology” (Revised edition) by Harry Henderson. Infobase Publishing, 2009
14. “Flight of the Robobee: the Rise of Swarm Robotics” by Tim Smedley. http://www.theguardian.com/sustainable-business/swarm-robotics-conservation-coral-reefs-pollination
15. “From ENIAC to Everyone: Talking with J. Presper Eckert” by Alexander Randall. http://www.kurzweilai.net/articles/art0645.html
16. ‘Fuzzy Logic: Четкие решения нечеткой логики.” http://www.bacnet.ru/knowledge-base/articles/index.php?ELEMENT\_ID=653
17. “History of Programming Languages-II” by Thomas J. Bergin and Richard G. Gibson. New York: ACM Press, 1996.
18. “How Quantum Cryptology Works” by Josh Clark. science.howstuffworks.com/.../quantum-cryptology.htm
19. http://albatron.ru/27-kompyuter-na-parovoj-tyage-ili-o-tvorenii-britanskix-uchenyx.html
20. http://gimn6.ru/article.asp?id\_text=60
21. http://globalfuturist.com/about-igf/top-ten-trends/top-ten-computer-trends-for-the-21st-century.html
22. http://shkolazhizni.ru/archive/0/n-37499/
23. http://software-security.sans.org/resources/paper/cissp/overview-tutorial-artificial-intelligence-systems
24. http://thinkinnovative.ru/experts/blogs/id/78
25. http://www.dataved.ru/2013/01/slang-is-difficult-for-ibm.html
26. “Introduction to Artificial Intelligence” by Wolfgang Ertel. Springer-Verlag London Limited, 2011
27. “Introduction to Information Security” by Linda Pesante. Carnegie Mellon University, 2008
28. “The Art of Computer Programming: Semi-numerical Algorithms” by Donald E. Knuth. Addison-Wesley; 1981
29. [Landofcode.com](http:///h) Webhostinggeeks.com Institut fur Theoretische Physik [http://www.itp.uni-hannover.de/?lang=en](http:///h)
30. Megaspring.ucoz.ru http://www.ozon.ru/context/detail/id/1421843/
31. “Operating System Concepts” (8th edition) by Silberschats, Galvin, Gagne. John Wiley & Sons Inc., 2008
32. “Organization and Architecture. Designing for Performance” by William Stallings. Pearson Prentice Hall, 2010
33. “Past, Present, and Future Methods of Cryptography and Data Encryption” A Research Review by Nicholas G. McDonald. Department of Electrical and Computer Engineering, University of Utah
34. “Programming Languages”. McGraw-Hill Encyclopedia of Science and Technology. New York: McGraw-Hill, 1997.
35. “Quantum Cryptography” by Alves, Carolina Moura and Kent Adrian. National University of Singapore. http://www.quantumlah.org/?q=tutorial/quantumcrypto
36. “Quantum Cryptography Tutorial” Dartmouth College. http://www.cs.dartmouth.edu/~jford/crypto.html
37. “Quantum Cryptography: Privacy through Uncertainty” by Salvatore Vittorio. Proquest - CSA - October 2002. http://www.csa.com/discoveryguides/crypt/overview.php
38. “Quantum Programming Languages: Survey and Bibliography” by Simon J. Gay. Department of Computing Science, University of Glasgow, Glasgow G12 8QQ, UK , 2006
39. “Security of the Internet” by James Ellis, Howard F. Lipson, Thomas A. Longstaff, Linda Pesante, Derek Simmel. NEWS AT SEI, 1998.
40. “Tales of the Encrypted” by Brodney A, Asher J. http://library.thinkquest.org/28005/flashed/index2.shtml.
41. “The Codebreakers: The Story of Secret Writing” by D. Kahn. Scribner, 1996.
42. “The ENIAC Story” by Martin H. Weik. Ordnance Ballistic Research Laboratories, Aberdeen Proving Ground, MD ftp.arl.mil/mike/comphist/eniac-story.html
43. to.prabc.ru
44. transhumanism-russia.ru
45. “Understanding Programming Languages” by M. Ben-Ari Weizmann. Institute of Science. Originally published by John Wiley & Sons, Chichester, 1996.
46. “Web Graphics for Dummies” by Linda Richards. Wiley/Dummies, 1997*.*
47. “What is Artificial Life?” http://www.wisegeek.com/what-is-artificial-life.htm
48. “What is Swarm Robotics? “ http://www.wisegeek.com/what-is-swarm-robotics.htm
49. www.book.kbsu.ru
50. www.ccas.ru
51. www.inf1.info/machineneumann
52. www.osp.ru
53. “Ионы для квантовых компьютеров.” Кристофер Монро, Дэвид Уайнленд, «В мире Науки», ноябрь, 2008
54. “Квантовая криптография.” Курсовая работа по дисциплине: Криптография. Кафедра Информационной безопасности, Студент группы Зи91 Лазарев Ю.А. МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ИНСТИТУТ ЭЛЕКТРОНИКИ И МАТЕМАТИКИ (технический университет), МОСКВА 2003.
55. “Легенда о Сетуни” http://habrahabr.ru/post/46688/
56. “Московский университет”, №31, октябрь, 2008
57. “[Основные понятия - Криптография](http:///h)” kriptografea.narod.ru/osnponiatia.html
58. “Первая ЭВМ” http://info61.blogspot.ru/p/20-1902-3-1974-1953-12.html
59. “[Современные биометрические методы идентификации.”](https://www.google.ru/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&sqi=2&ved=0CD8QFjAC&url=http%3A%2F%2Fhabrahabr.ru%2Fpost%2F126144%2F&ei=cfWJU8mPI8r54QT91oCIDg&usg=AFQjCNF5CmBIEfhlTgCWD8hFmhw9x8auFQ&sig2=f5I9qCaVrZkGIwUdpgpv-A&bvm=bv.67720277,d.bGE&cad=rjt) habrahabr.ru/post/126144/11 авг. 2011

**CONTENTS**

[**HISTORY OF COMPUTING** 5](#_Toc391908873)

[**PRE-COMPUTER ERA** 5](#_Toc391908874)

[**EARLY COMPUTERS** 11](#_Toc391908875)

[**1950s - PRESENT DAY: DECADE BY DECADE GUIDE** 18](#_Toc391908876)

[**COMPUTING COMPONENTS. THE VON NEUMANN ARCHITECTURE.** 31](#_Toc391908877)

[**ARCHITECTURE AND ORGANIZATION** 31](#_Toc391908878)

[**STRUCTURE AND FUNCTIONS** 36](#_Toc391908879)

[**SECONDARY STORAGE DEVICES** 43](#_Toc391908880)

[**PROGRAMMING LANGUAGES AND PROGRAM LANGUAGE CONCEPTS** 51](#_Toc391908881)

[**BRIEF HISTORY OF COMPUTER PROGRAMMING LANGUAGES** 51](#_Toc391908882)

[**GENERATIONS OF LANGUAGES** 63](#_Toc391908883)

[**PROGRAMMING LANGUAGE APPLICATIONS** 69](#_Toc391908884)

[**BASIC TYPES OF PROGRAMMING LANGUAGES** 74](#_Toc391908885)

[**LANGUAGE EVALUATION CRITERIA. IMPLEMENTATION METHODS** 85](#_Toc391908886)

[**OPERATING SYSTEMS** 91](#_Toc391908887)

[**DEVELOPMENT** 93](#_Toc391908888)

[**FUNCTIONS** 97](#_Toc391908889)

[**EXAMPLES OF OPERATING SYSTEMS** 108](#_Toc391908890)

[**INTERNET** 117](#_Toc391908891)

[**E-MAIL** 124](#_Toc391908892)

[**WORLD WIDE WEB** 128](#_Toc391908893)

[**WEB BROWSER** 134](#_Toc391908894)

[**WEB PAGE DESIGN** 142](#_Toc391908895)

[**INTERNET PROTOCOLS** 148](#_Toc391908896)

[**COMPUTER SECURITY AND RISKS** 154](#_Toc391908897)

[**BASIC COMPUTER SECURITY CONCEPTS** 154](#_Toc391908898)

[**TYPES OF INCIDENTS** 159](#_Toc391908899)

[**IMPROVING SECURITY** 166](#_Toc391908900)

[**BIOMETRIC SECURITY TECHNOLOGY** 172](#_Toc391908901)

[**CRYPTOGRAPHY AND** **DATA ENCRYPTION** 181](#_Toc391908902)

[**TERMINOLOGY** 181](#_Toc391908903)

[**HISTORICAL CRYPTOGRAPHY** 185](#_Toc391908904)

[**MODERN ENCRYPTION** 193](#_Toc391908905)

[**FUTURE METHODS OF ENCRYPTION** 200](#_Toc391908906)

[**COMPUTER GRAPHICS** 207](#_Toc391908907)

[**HISTORY AND DEVELOPMENT** 207](#_Toc391908908)

[**CONCEPTS AND PRINCIPLES** 212](#_Toc391908909)

[**IMAGE TYPES** 218](#_Toc391908910)

[**ARTIFICIAL INTELLIGENCE: OVERVIEW** 225](#_Toc391908911)

[**DEFINITIONS** 225](#_Toc391908912)

[**APPROACHES AND TECHNIQUES** 231](#_Toc391908913)

[**CURRENT TRENDS** 239](#_Toc391908914)

[**ARTIFICIAL INTELLIGENCE: ROBOTICS AND A-LIFE** 246](#_Toc391908915)

[**ROBOTICS** 246](#_Toc391908916)

[**ARTIFICIAL LIFE** 256](#_Toc391908917)

[**FUTURE COMPUTING** 267](#_Toc391908918)

[**QUANTUM COMPUTING** 267](#_Toc391908919)

[**BIOINFORMATICS** 271](#_Toc391908920)

[**NANOTECHNOLOGY** 277](#_Toc391908921)

[**UBIQUITOUS COMPUTING** 281](#_Toc391908922)

[**SUPERCOMPUTERS** 285](#_Toc391908923)

[**LITERATURE** 292](#_Toc391908924)