

ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ

для проведения промежуточной аттестации

по учебной дисциплине

**ОГСЭ.04 ИНОСТРАННЫЙ ЯЗЫК В ПРОФЕССИОНАЛЬНОЙ
ДЕЯТЕЛЬНОСТИ (АНГЛИЙСКИЙ)**

программы подготовки специалистов среднего

для специальности

13.02.11 Техническая эксплуатация и обслуживание электрического и
электромеханического оборудования (по отраслям)

Форма проведения оценочной процедуры

дифференцированный зачет

СОГЛАСОВАНО

зав. по УМР

 Н.А. Ивашкина

27 августа 2020 года

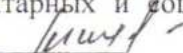
Фонды оценочных средств учебной дисциплины разработаны на основе:

- ✓ Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования (далее – СПО) 13.02.11 Техническая эксплуатация и обслуживание электрического и электромеханического оборудования (по отраслям), утвержденного приказом Минобрнауки России от 07.12.2017 года, зарегистрирован в Минюсте России 21.12.2017 года, укрупненная группа специальностей 13.00.00 Электро- и теплоэнергетика;
- ✓ примерной основной образовательной программы по специальности 13.02.11 Техническая эксплуатация и обслуживание электрического и электромеханического оборудования (по отраслям)

Организация-разработчик: государственное бюджетное учреждение Калининградской области профессиональная образовательная организация «Технологический колледж»

Разработчик:

Андрিয়াускайте И.А., преподаватель первой квалификационной категории

Рассмотрены на заседании методической кафедры «Общегуманитарных и социально-экономических дисциплин». Протокол №1 от 27 августа 2020 года 

Рекомендованы методическим советом государственного бюджетного учреждения Калининградской области профессиональной образовательной организацией «Технологический колледж». Протокол №01 от 28 августа 2020 года

1. Паспорт фонда оценочных средств

1.1 Область применения фонда оценочных средств

Фонд оценочных средств (ФОС) предназначены для оценки результатов освоения учебной дисциплины ОГСЭ.04 Иностранный язык в профессиональной деятельности (Английский). ФОС включает контрольные материалы для проведения промежуточной аттестации в форме дифференцированного зачета.

Код ПК, ОК	Умения	Знания
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	Приемы аннотирования, реферирования и перевода специализированной литературы по профилю подготовки. Лексика по профилю подготовки.
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	Чтение, письмо, восприятие речи на слух и воспроизведение иноязычного текста по ключевым словам или по плану. Приемы структурирования информации.
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие.	Способы самостоятельной оценки и совершенствования уровня знаний по иностранному языку. Особенности произношения на иностранном языке. Возможные траектории профессионального развития и самообразования.
ОК 04.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	Основы проектной деятельности. Основы эффективного сотрудничества в коллективе.
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	Правила устной и письменной коммуникации при переводе с иностранного языка. Лексика по профилю подготовки.
ОК 06.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	Основные правила поведения и речевого этикета в сферах повседневного, официально-делового и профессионального общения. Лексика в данной области.
ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	Правила экологической безопасности и ресурсосбережения при ведении профессиональной деятельности. Лексика в данной области.
ОК 08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе	Основы здорового образа жизни. Лексика в данной области.

	профессиональной деятельности и поддержание необходимого уровня физической подготовленности.	
ОК 09.	Использовать информационные технологии в профессиональной деятельности.	Современные средства и устройства информатизации и их использование. Правила работы на компьютере и оргтехнике. Правила ведения переписки по электронной почте.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языке.	Правила чтения текстов профессиональной направленности на иностранном языке. Правила построения простых и сложных предложений на профессиональные темы. Основные общеупотребительные глаголы. Лексика, относящаяся к описанию предметов, средств и процессов профессиональной деятельности. Правила оформления документов.
ОК 11.	Планировать предпринимательскую деятельность в профессиональной сфере.	Лексический минимум и нормы речевого поведения и делового этикета для построения устной и письменной речи на иностранном языке. Правила ведения деловой переписки. Работа с бизнес статьями на иностранном языке с целью извлечения и переработки информации, ведения переговоров в деловой среде.
ПК 1.1	Анализировать техническое задание на разработку конструкции типовых деталей, узлов изделия и оснастки.	Перевод со словарём основной терминологии по профилю подготовки.
ПК 1.4	Применять информационно-коммуникационные технологии для обеспечения жизненного цикла технической документации.	Перевод со словарём основной терминологии по профилю подготовки. Правила оформления документов.
ПК 2.1	Анализировать конструкторскую документацию.	Перевод, обобщение и анализ специализированной литературы по профилю подготовки.
ПК 4.2	Применять информационно-коммуникационные технологии при сборе, обработке и хранении технической, экономической и других видов информации.	Приемы аннотирования, реферирования и перевода специализированной литературы по профилю подготовки.

Формы и методы оценивания

Предметом оценки служат умения и знания, предусмотренные ФГОС по дисциплине ОГСЭ.04 Иностранный язык в профессиональной деятельности (Английский), направленные на формирование знаний, умений

Результаты обучения	Критерии оценки	Методы оценки
<p>Знания: Лексика по профилю подготовки. Приемы аннотирования, реферирования и перевода специализированной литературы по профилю подготовки. Приемы структурирования информации. Способы самостоятельной оценки и совершенствования уровня знаний по иностранному языку. Особенности произношения на иностранном языке. Возможные траектории профессионального развития и самообразования. Основы проектной деятельности. Основы эффективного сотрудничества в коллективе. Правила устной и письменной коммуникации при переводе с иностранного языка. Основные правила поведения и речевого этикета в сферах повседневного, официально-делового и профессионального общения. Правила экологической безопасности и ресурсосбережения при ведении профессиональной деятельности. Основы здорового образа жизни. Современные средства и устройства информатизации и их использование. Правила работы на компьютере и оргтехнике. Правила ведения переписки по электронной почте. Правила чтения текстов профессиональной направленности на иностранном языке. Правила построения простых и сложных предложений на профессиональные темы. Основные общеупотребительные глаголы (бытовая и профессиональная лексика). Лексика, относящаяся к описанию предметов, средств и процессов профессиональной деятельности. Лексический минимум и нормы речевого поведения и делового этикета для построения устной и письменной речи на иностранном языке.</p>	<p>- не имеет базовых знаний (1); - допускает существенные ошибки при раскрытии содержания и особенностей употребления изученного материала (2); - демонстрирует частичное знание содержания и особенностей употребления изученного материала (3); - демонстрирует знание содержания и особенностей употребления изученного материала, но дает не полное его обоснование (4); - демонстрирует полное правильное знание содержания и особенностей употребления изученного материала, аргументировано обосновывает тот или иной выбор при выполнении практического задания (5).</p> <p>5</p>	<p>Входной контроль: тестирование</p> <p>Текущий контроль: устный опрос, беседа, сообщение, реферат, доклад, презентация, тестирование, контрольные работы</p> <p>Промежуточный контроль: дифференцированный зачет</p>

<p>Правила ведения деловой переписки. Правила оформления документов.</p>		
<p>Умения:</p> <ul style="list-style-type: none"> - понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые); - понимать тексты на базовые профессиональные темы; - участвовать в диалогах на знакомые общие и профессиональные темы; - строить простые высказывания о себе и о своей профессиональной деятельности; - кратко обосновывать и объяснить свои действия (текущие и планируемые); - писать простые связные сообщения на знакомые или интересующие профессиональные темы; - читать, писать, воспринимать речь на слух и воспроизводить иноязычный текст по ключевым словам или по плану; - работать с бизнес статьями на иностранном языке с целью извлечения и переработки информации, ведения переговоров в деловой среде; - переводить со словарём основные термины по профилю подготовки; - переводить, обобщать и анализировать специализированную литературу по профилю подготовки. 	<ul style="list-style-type: none"> - не умеет и не готов к взаимодействию на иностранном языке (1); - имея базовые знания, не умеет самостоятельно отбирать, систематизировать и применять усвоенную информацию для реализации чтения, письма, говорения и восприятия речи на слух на иностранном языке (2); - демонстрирует частичное владение чтением, письмом, говорением и восприятием речи на слух и допускает существенные ошибки при их реализации (3); - демонстрирует в целом успешное владение чтением, письмом, говорением и восприятием речи на слух, но допускает некоторые пробелы и неточности в конкретных заданных условиях(4); - демонстрирует правильное владение чтением, письмом, говорением и восприятием речи на слух на иностранном языке для обеспечения полноценной профессиональной деятельности (5). 	<p>Входной контроль: тестирование.</p> <p>Текущий контроль: устный опрос, беседа с экспертом, контрольные работы, тестирование, защита индивидуальных и групповых заданий проектного характера</p> <p>Промежуточный контроль: дифференцированный зачет</p>

1.3. Описание правил оформления результатов оценивания

Отметка	Правильных ответов по заданиям билета
«5»	Все задания с допущением 1-3 ошибок
«4»	Все задания с допущением 3-5 ошибок
«3»	Два из трех заданий билета с допущением не более 3-5 ошибок
«2»	Менее двух выполненных заданий

II. Фонды оценочных средств

2.1 Задания для оценки знаний и умений

Текст №1.

The Need for Network Security

The Internet continues to grow exponentially. Personal, government, and business applications continue to multiply on the Internet, with immediate benefits to end users. However, network-based applications and services can pose security risks to individuals and to the information resources of companies and governments. Information is an asset that must be protected.

Security has one purpose: to protect assets. For most of history, this meant building strong walls to stop the enemy and establishing small, well-guarded doors to provide secure access for friends. This strategy worked well for the centralized, fortress-like world of mainframe computers and closed networks.

The closed network typically consists of a network designed and implemented in a corporate environment and provides connectivity only to known parties and sites without connecting to public networks. Networks were designed this way in the past and thought to be reasonably secure because of no outside connectivity.

With the advent of personal computers, LANs, and the wide-open world of the Internet, the networks of today are more open. As e-business and Internet applications continue to grow, the key to network security lies in defining the balance between a closed and open network and differentiating the good guys from the bad guys.

With the increased number of LANs and personal computers, the Internet began to create untold numbers of security risks. Firewall devices, which are software or hardware that enforce an access control policy between two or more networks, were introduced. This technology gave users a balance between security and simple outbound access to the Internet, which was mostly used for e-mail and web surfing.

This balance was short-lived as the use of extranets began to grow, which connected internal and external business processes. Businesses were soon realizing tremendous cost savings by connecting supply-chain management and enterprise resource planning systems to their business partners, and by connecting sales-force automation systems to mobile employees, and by providing electronic commerce connections to business customers and consumers. The firewall began to include intrusion detection, authentication, authorization, and vulnerability-assessment systems. Today, successful companies have again struck a balance by keeping the enemies out with increasingly complex ways of letting friends in.

Most people expect security measures to ensure the following:

- Users can perform only authorized tasks.
- Users can obtain only authorized information.

Users cannot cause damage to the data, applications, or operating environment of a system.

The word *security* means protection against malicious attacks by outsiders and by insiders. Statistically, there are more attacks from inside sources.

Security also involves controlling the effects of errors and equipment failures. Anything that can protect against an attack will probably prevent random misfortunes, too.

Exercise 1. *Answer the questions using the information from the text.*

1. Who can be put at risk by network-based applications?
2. What strategy was effective in the period of mainframe computers and closed networks?
3. What is a closed network?
4. What is considered to be the key to network security nowadays?
5. How do firewall devices benefit users?
6. What advantages does connecting internal and external business processes give to companies?
7. What functions do firewall devices need as a result of growing use of extranets?
8. What do most people expect from security measures?
9. What does network security involve except for protection against malicious attacks?

Exercise 2. *True or false?*

1. The firewall device is used to prevent connecting to public networks.
2. The use of extranets gave businesses a lot of new opportunities.
3. The Internet became more secure when the number of personal computers increased.
4. Vulnerability-assessment systems cannot be included into firewall devices.
5. Networks are more often attacked by insiders than by outsiders.

Exercise 3. *Write a short summary of the text.*

Exercise 4. *Use the words and expressions from the box to complete the sentences.*

vulnerability-assessment connectivity public network authorization e-business
 application firewall authentication LAN access

1. Before connecting to a _____, make sure your system is fully up to date with the latest patches.
2. End users have great difficulty using this file permission system to create security policies for file _____.
3. _____ is the process of determining whether someone or something is, in fact, who or what it is declared to be.
4. _____ is the process used in verifying that someone who has requested or initiated an action has the right to do so.
5. _____ is capable of transmitting data at very fast rates, much faster than data can be transmitted over a telephone line; but the distances are limited and there is also a limit on the number of computers that can be attached to it.
6. Sometimes a new and popular _____ arises which only runs on one platform, increasing the desirability of that platform.
7. If security holes are found as a result of _____, a vulnerability disclosure may be required.
8. When organizations go online, they have to decide which _____ models best suit their goals.
9. Persistent _____ is impossible in a mobile world, which means it is also impossible for employees to access their enterprise applications when they need them most—when they're in the field doing their jobs.
10. When a packet passes through a _____, it filters the packet on a protocol/port number basis.

Exercise 5. *Match the verbs and the nouns. Sometimes, more than one option is possible.*

1. surf
 2. provide
 3. connect to
 4. perform
 5. cause
-
- a. task
 - b. access
 - c. the web
 - d. damage
 - e. a network

Время выполнения - 45 минут.

Критерии оценки:

Правильно выполненное задание – 5 баллов.

Всего 20 баллов.

Критерии оценивания:

Количество правильных ответов	Процент выполнения	Оценка
-------------------------------	--------------------	--------

18 – 20	90 % - 100%	5 (отлично)
16 – 17	80% - 89%	4 (хорошо)
14 - 15	70 % - 79%	3 (удовлетворительно)
менее 14	менее 70%	2 (не удовлетворительно)

Текст № 2

Attacks

Four primary classes of attacks exist: (1) reconnaissance, (2) access, (3) denial of service, and (4) worms, viruses, and Trojan horses.

Reconnaissance is an unauthorized discovery and mapping of systems, services, or vulnerabilities. It is also known as information gathering and, in most cases, it precedes an actual access or denial-of-service attack. Reconnaissance is somewhat analogous to a thief casing a neighborhood for vulnerable homes to break into, such as an unoccupied residence, easy-to-open doors, or open windows.

System access is the ability for an unauthorized intruder to gain access to a device for which the intruder does not have an account or a password. Entering or accessing systems to which one does not have authority to access usually involves running a hack, script, or tool that exploits a known vulnerability of the system or application being attacked.

Denial of service (DoS) implies that an attacker disables or corrupts networks, systems, or services with the intent to deny services to intended users. DoS attacks involve either crashing the system or slowing it down to the point that it is unusable. But DoS can also be as simple as deleting or corrupting information. In most cases, performing the attack simply involves running a hack or script. The attacker does not need prior access to the target because a way to access it is all that is usually required. For these reasons, DoS attacks are the most feared.

Malicious software (worms, viruses, and Trojan horses) is inserted onto a host to damage a system; corrupt a system; replicate itself; or deny services or access to networks, systems or services. They can also allow sensitive information to be copied or echoed to other systems.

Trojan horses can be used to ask the user to enter sensitive information in a commonly trusted screen. For example, an attacker might log in to a Windows box and run a program that looks like the true Windows logon screen, prompting a user to type his username and password. The program would then send the information to the attacker and then give the Windows error for bad password. The user would then log out, and the correct Windows logon screen would appear; the user is none the wiser that his password has just been stolen.

Even worse, the nature of all these threats is changing—from the relatively simple viruses of the 1980s to the more complex and damaging viruses, DoS attacks, and hacking tools in recent years. Today, these hacking tools are powerful and widespread, with the new dangers of selfspreading blended worms and network DoS attacks. Also, the old days of attacks that take days or weeks to spread are over. Threats now spread worldwide in a matter of minutes.

The next generations of attacks are expected to spread in just seconds. These worms and viruses could do more than just wreak havoc by overloading network resources with the amount of traffic they generate, they could also be used to deploy damaging payloads that steal vital information or erase hard drives. Also, there is a strong concern that the threats of tomorrow will be directed at the very infrastructure of the Internet.

Exercise 1. *Answer the questions using the information from the text.*

1. What is a common classification of attacks?
2. What are the objectives of reconnaissance?
3. When can accessing a system be considered an attack?
4. What do DoS attacks usually involve?
5. What examples of malicious software exist?
6. What damage is malicious software able to cause to a system?

7. How can Trojan horses be used to steal passwords?
8. How are attacks changing over the time?
9. What are the next generations of attacks expected to be like?

Exercise 2. *True or false?*

1. Reconnaissance is often used as the first step of a major attack.
2. DoS attacks are dangerous because most of them are very simple to perform.
3. Viruses spread considerably faster nowadays than before.
4. Selfspreading blended worms originate from the 1980s.
5. The next generations of attacks could erase hard drives.

Exercise 3. *Write a short summary of the text.*

Exercise 4. *Use the words and expressions from the box to complete the sentences.* malicious software password denial of service reconnaissance worm payload logon screen hard drive username intruder

1. Windows makes it possible to change the _____ that appears when you start your computer without any third-party software, but this setting is well hidden.
2. A _____ attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have.
3. The _____ detection technique tries to identify people behind attacks by analyzing their computational behaviour.
4. Nowadays, it is a common practice for computer systems to hide a _____ as it is typed.
5. Spyware or other _____ is sometimes found embedded in programs supplied officially by companies, e.g., downloadable from websites, that appear useful or attractive, but may have, for example, additional hidden tracking functionality that gathers marketing statistics.
6. In a computer, a _____ is a self-replicating virus that does not alter files but resides in active memory and duplicates itself.
7. Your _____ can be used to create a custom link to your profile that you can give out to people or post on external websites.
8. Active _____ is a type of computer attack in which an intruder engages with the targeted system to gather information about vulnerabilities.
9. In computer security, _____ refers to the part of malware which performs a malicious action.
10. Computers have a _____ and use it to store files for the operating system and software that run on the computer, as well as files created or downloaded to the computer by a user.

Exercise 5. *Match the verbs and the nouns. Sometimes, more than one option is possible.*

1. deny
2. type
3. map
4. erase
5. deploy

- a. a hard drive
- b. a payload
- c. a username
- d. a service
- e. a system

Критерии оценки:

Правильно выполненное задание – 5 баллов.

Всего 20 баллов.

Критерии оценивания:

Количество правильных ответов	Процент выполнения	Оценка
18 – 20	90 % - 100%	5 (отлично)
16 – 17	80% - 89%	4 (хорошо)
14 - 15	70 % - 79%	3 (удовлетворительно)
менее 14	менее 70%	2 (не удовлетворительно)

Текст № 3.

Software Security

Software security is the idea of engineering software so that it continues to function correctly under malicious attack. Most technologists acknowledge this undertaking's importance, but they need some help in understanding how to tackle it.

A central and critical aspect of the computer security problem is a software problem. Software defects with security ramifications—including implementation bugs such as buffer overflows and design flaws such as inconsistent error handling—promise to be with us for years. All too often, malicious intruders can hack into systems by exploiting software defects. Internet-enabled software applications present the most common security risk encountered today, with software's ever-expanding complexity and extensibility adding further fuel to the fire.

Pondering the question, "What is the most effective way to protect software?" can help untangle software security and application security. On one hand, software security is about building secure software: designing software to be secure, making sure that software is secure and educating software developers, architects and users about how to build secure things. On the other hand, application security is about protecting software and the systems that software runs in a post facto way, after development is complete. Issues critical to this subfield include sandboxing code (as the Java virtual machine does), protecting against malicious code, obfuscating code, locking down executables, monitoring programs as they run (especially their input), enforcing the software use policy with technology and dealing with extensible systems.

Application security follows naturally from a network-centric approach to security, by embracing standard approaches such as penetrate and patch and input filtering (trying to block malicious input) and by providing value in a reactive way. One reason that application security technologies such as firewalls have evolved the way they have is because operations people dreamed them up. In most corporations and large organizations, security is the domain of the infrastructure people who set up and maintain firewalls, intrusion detection systems, and antivirus engines (all of which are reactive technologies).

However, these people are operators, not builders. Given the fact that they don't build the software they have to operate, it's no surprise that their approach is to move standard security techniques "down" to the desktop and application levels. The gist of the idea is to protect vulnerable things (in this case, software) from attack, but the problem is that vulnerabilities in the software let malicious hackers skirt standard security technologies with impunity. If this were not the case, then the security vulnerability problem would not be expanding the way that it is. Clearly, this emphasizes the need to get builders to do a better job on the software in the first place.

On the road to making such a fundamental change, we must first agree that software security is not security software. This is a subtle point often lost on development people who tend to focus on functionality. Obviously, there are security functions, and most modern software includes security

features, but adding features such as SSL (for cryptographically protecting communications) does not present a complete solution to the security problem. Software security is a system-wide issue that takes into account both security mechanisms (such as access control) and design for security (such as robust design that makes software attacks difficult). Software security must be part of a full life cycle approach. Just as you can't test quality into a piece of software, you can't spray paint security features onto a design and expect it to become secure. There's no such thing as a magic crypto fairy dust—we need to focus on software security from the ground up.

Exercise 1. *Answer the questions using the information from the text.*

1. How can the concept of software security be described?
2. Why is software the central aspect of computer security?
3. What does software security involve?
4. What does application security involve?
5. What standard approaches of application security exist?
6. Why do application security techniques prevail nowadays?
7. Why do not application security techniques always work well?
8. What is the difference between software security and security software?
9. When should software developers start focusing on security?

Exercise 2. *True or false?*

1. Engineering secure software is a complicated issue for most technologists.
2. The problem of implementation bugs is likely to be solved in the short term.
3. Internet-enabled software applications are relatively secure.
4. The more complex software is, the less risk it presents.
5. Modern software should never include security features.

Exercise 3. *Write a short summary of the text.*

Exercise 4. *Use the words and expressions from the box to complete the sentences.*

executable desktop use policy buffer overflow sandbox bug full life cycle antivirus engines robust design design flaws

1. Here are some examples of _____: broken authentication mechanism (that could be authentication bypass), failure to authorize after authentication, not explicitly validating all data or understanding how integrated external components change the attack surface.
2. A _____ is a set of rules applied by the owner, creator or administrator of a network, website, or service, that restrict the ways in which the network, website or system may be used, and sets guide lines as to how it should be used.
3. Multiscanning is running multiple anti-malware or _____ concurrently.
4. In Windows operating system, an _____ usually has a file name extension of .bat, .com, or .exe.
5. Systems development life cycle (SDLC) and systems analysis and design (SAD) are cornerstones of _____ product and system planning.
6. _____ is a set of engineering methods widely successful in reducing sensitivity to such noise factors as customer use conditions, manufacturing variability, and degradation of a system over time.
7. In general, a _____ is an isolated computing environment in which a program or file can be executed without affecting the application in which it runs.
8. A _____ occurs when a program or process tries to store more data in a temporary data storage area than it was intended to hold.
9. If an inconsistency is encountered, the program may immediately halt so that the _____ may be located and fixed.
10. An all-in-one _____ computer typically combines the case and monitor in one unit.

Exercise 5. Match the verbs and the nouns. Sometimes, more than one option is possible.

filter
handle
run
enter
detect

a system
information
an error
an intrusion
input

Время выполнения - 45 минут.

Критерии оценки:

Правильно выполненное задание – 5 баллов.

Всего 20 баллов.

Критерии оценивания:

Количество правильных ответов	Процент выполнения	Оценка
18 – 20	90 % - 100%	5 (отлично)
16 – 17	80% - 89%	4 (хорошо)
14 - 15	70 % - 79%	3 (удовлетворительно)
менее 14	менее 70%	2 (не удовлетворительно)

Текст № 4.

Government to Rescue IT?

Internet and computer growth in Russia has been the envy of every European and North American country during the past few years. But growth in all IT areas is expected to slow by a considerable amount. Cell-phone growth in Moscow and St.Petersburg is limited to subscribers exchanging models, while subscriber growth is limited to the regions. Mobile communication companies had hoped that 3G technology would prove to be a boom, but the lack of equipment capable of handing such a technology is holding back development.

“Informatization” of the country means simply buying more computers and increasing. Internet usage has nearly reached the limit that current technological equipment can provide. There is not enough money to increase capacity. The largest computer and Internet service providers in Russia will reach yearly turnover of \$500 million, which is far too small of a sum to begin improving communication structures on their own.

Moreover, Russian IT faces another problem: most of the people who need computers live in cities of one million or more, and those people have already bought them. The majority who live outside of “wired” urban areas have absolutely no reason to buy a computer.

The government, did launch the Electronic Russian program, which was designed to create an electronic government that would increase interaction between citizens and their elected leaders. Different ministries and political organs could not agree on how to implement the program, and it came to nothing. The government has developed a new plan. This time a single ministry will be responsible for “ informatization”, and its decisions will be carried out by all government organs. The

IT created office will have to have not only the necessary resources but also a fair share of political leverage. If this is not done, then Russia will have to wait many years for IT businesses to become large enough to put pressure on the government to “informatize”.

The most popular Internet service is e-mail. Most of the people, who have access to the Internet, use the network only for sending and receiving e-mail messages. However, other popular services are available on the Internet: reading USENET News, using the World-Wide Web, telnet, FTP, and Gopher.

In many developing countries the Internet may provide businessmen with a reliable alternative to the expensive and unreliable telecommunications systems of these countries. Commercial users can communicate over the Internet with the rest of the world and can do it very cheaply. When they send e-mail messages, they only have to pay for phone calls to their local service providers, not for calls across their countries or around the world. But who actually pays for sending e-mail messages over the Internet long distances, around the world? The answer is very simple: user pays his/her service provider a monthly or hourly fee. Part of this fee goes towards its costs to connect to a larger service provider. Part of the fee got by the larger provider goes to cover its cost of running a worldwide network of wires and wireless stations.

Задания к тексту

Прочитайте текст и переведите первые три абзаца на русский язык.

Найдите в тексте предложения, содержащие нижеследующие слова и выражения:

- a) mobile communication
- b) e-mail messages
- c) a service provider
- d) a worldwide network
- e) the World-Wide Web
- f) a local service provider
- g) a wireless station

Соотнесите следующие ключевые слова с соответствующим переводом:

- | | |
|--------------------------------------|--|
| 1) Internet growth | a) компьютерный рост |
| 2) a considerable amount | b) электронная программа |
| 3) a current technological equipment | c) компании мобильных структур |
| 4) Increasing Internet usage | d) распространение компьютеров |
| 5) mobile communication companies | e) структуры связи |
| 6) communication structures | f) доступ в интернет |
| 7) spreading computers | g) увеличение Интернет обращения |
| 8) Internet access | h) поток технологического оборудования |
| 9) a computer growth | i) значительное количество |
| 10) an electronic program | j) расширение Интернета |

Грамматическое задание:

1. The old man's clothes ... torn.

- a) was c) were
- b) is d) has been

2. We mustn't climb the mountain, ... we?

- a) can c) mustn't
- b) can't d) must

14

3. The President ... a fund for the homeless.

- a) found c) founds
- b) finds d) founded

4. He draws extremely

- a) good c) well
 b) bad d) fine
5. If I ... a millionaire, I'll give lots of money to the poor.
 a) be c) become
 b) is d) are
6. Shall I throw ... coffee away?
 a) a c) these
 b) an d) this
7. Some people like summer best, some like spring or autumn, ... prefer winter.
 a) another c) the others
 b) the other d) others
8. Hey, Jack! How are you getting ... ? – Fine, thanks.
 a) of c) on
 b) off d) over
9. Well, girls, who is going to ... the table for tea?
 a) lay c) laid
 b) He d) lain
10. Nobody likes to be cheated, ... he?
 a) doesn't c) is
 b) does d) isn't

Выберите правильный вариант перевода.

- 1) «Incorrect number of parameters»
 а) неверные параметры
 б) неверное количество параметров
 в) неверный номер параметров
- 2) «Bad command or file name»
 а) неверная команда и имя файла
 б) неверная команда и файл имени
 в) неверная команда или имя файла
- 3) «Insufficient disk space»
 а) достаточно места на диске
 б) не достаточно места на диске
 в) диск достаточного объёма
- 4) «No room for system on destination disk»
 а) нет места для системы на диске, на который осуществляется копирование
 б) нет пространственной системы на диске, на который осуществляется копирование
 в) не помещайте систему на диск, на который осуществляется копирование
- 5) «Syntax error»
 а) синтаксическая ошибка
 б) ошибочный синтаксис
 в) ошибки в синтаксисе
- 6) «Keyboard system» 15
 а) системная клавиатура
 б) система клавиатуры
 в) клавиатура в системе

- 7) «Read error in the file “x”»
а) читайте файл“x”
б) неверное чтение файла”x”
в) ошибка при чтении файла “x”

Выберите правильный перевод слова

1) «Клавиша»

- а) drive
б) port
в) root
г) key
д) mouse

2) «Память»

- а) error
б) message
в) memory
г) mouse
д) name

3) «Имя»

- а) character
б) key
в) port
г) mouse
д) name

4) «Порт»

- а) keyboard
б) drive
в) mouse
г) port
д) file

5) «Корневой»

- а) hard
б) floppy
в) personal
г) root
д) display

6) «Дисковод»

- а) drive
б) diskette
в) disk
г) port
д) screen

7) «Экран»

- а) display
б) keyboard
в) memory

- г) error
- д) screen

- 8) «Ошибка»
- а) message
 - б) root
 - в) port
 - г) printer
 - д) error

- 9) «Программное обеспечение»
- а) hardware software
 - б) program
 - в) software
 - г) command
 - д) character
 - е) message

- 10) «Место»
- а) usage
 - б) enough
 - в) such
 - г) warning
 - д) room

Переведите. Выберите правильный вариант ответа.

1. Электронная цифровая подпись это

- аналог собственноручной подписи, являющийся средством защиты информации*
- документ, пригодный для автоматического считывания содержащейся в нём информации
- единый механизм по работе с документами, представленными в электронном виде
- составление номенклатуры документов, формирование справочников и классификаторов, составление инструкций

2. Под искусственным интеллектом обычно понимают

- способности компьютерных систем к таким действиям, которые назывались бы интеллектуальными, если бы исходили от человека*
- класс пакетов включает: информационные системы, поддерживающие диалог на естественном языке
- способности, связанные с человеческим мышлением
- интеллектуальные пакеты прикладных программ, позволяющие решать прикладные задачи без программирования

3. Компьютерные вирусы – это...

- файлы, имеющие определенное расширение
- программы, способные к саморазмножению (самокопированию)*
- программы, сохраняющиеся в оперативной памяти после выключения компьютера
- файлы, которые невозможно удалить

Текст № 5.

The Development of the Computers in the USA

In the early 1960's, when computers were hulking mainframes that took up entire rooms, engineers were already toying with the then – extravagant notion of building a computer intended for the sole use of one person, by the early 1970s, researchers at Xerox's Palo Alto Research Center (Xerox PARC) had realized that the pace of improvement in the technology of semiconductors – the chips of silicon that are the building blocks of present – day electronics – meant that sooner or later the PC would be extravagant no longer. They foresaw that computing power would someday be so cheap that engineers would be able to afford to devote a great deal of it simply to making non-technical people more comfortable with these new information-handling tools, in their labs, they developed or refined much of what constitutes PCs today, from “mouse” pointing devices to software “windows”.

Although the work at Xerox PARC was crucial, it was not the spark that took PCs out of the hands of experts and into the popular imagination. That happened in January 1975, when the magazine Popular Electronics put a new kit for hobbyists, called the Altair, on its cover, for the first time, anybody with \$400 and a soldering iron could buy and assemble his own computer. The Altair inspired Steve Wozniak and Steve Jobs to build the first Apple computer, and a young college dropout named Bill Gates to write software for it. Meanwhile, the person who deserves the credit for inventing the Altair, an engineer named Ed Roberts, left the industry he had spawned to go to medical school. Now he is a doctor in a small town in central Georgia.

To this day, researchers at Xerox and elsewhere pooh-poo the Altair as too primitive to have made use of the technology they felt was needed to bring PCs to the masses. In a sense, they are right. The Altair incorporated one of the first single-chip microprocessors – a semiconductor chip, that contained all the basic circuits needed to do calculations – called the Intel 8080. Although the 8080 was advanced for its time, it was far too slow to support the mouse, windows, and elaborate software Xerox had developed. Indeed, it wasn't until 1984, when Apple Computer's Macintosh burst onto the scene, that PCs were powerful enough to fulfill the original vision of researchers.

Researchers today are proceeding in the same spirit that motivated Kay and his Xerox PARC colleagues in the 1970s: to make information more accessible to ordinary people. But a look into today's research labs reveals very little that resembles what we think of now as a PC. For one thing, researchers seem eager to abandon the keyboard and the monitor that are the PC's trademarks. Instead they are trying to devise PCs with interpretive powers that are more humanlike – PCs that can hear you and see you, can tell when you're in a bad mood and know to ask questions when they don't understand anything

Задания к тексту:

1. Прочитайте текст и переведите первые два абзаца на русский язык .

2. Найдите в тексте предложения, содержащие нижеследующие слова и выражения:

- a) hulking mainframes
- b) a pace of improvement in the technology
- c) computing power
- d) non – technical people
- e) researchers of Xerox
- f) the first single-chip microprocessor
- g) to do calculations

3. Соотнесите следующие ключевые слова с соответствующим переводом:

- | | |
|-----------------------------------|--------------------------------|
| 1) a microprocessor | a) ручное управление |
| 2) to do calculations | 18 b) эксперт |
| 3) to motivate | c) электроника |
| 4) an invention | d) технология полупроводимости |
| 5) electronics | e) клавиатура |
| 6) a technology of semiconductors | f) компьютерная мощь |

- 7) a keyboard
- 8) an expert
- 9) handling tool
- 10) computing power

- g) изобретение
- h) побуждать
- i) микропроцессор
- j) делать вычисления

Грамматическое задание

1. He used ... in a bank.

- a) work
- b) to work
- c) working
- d) to working

2. What ... shame you could not join us!

- a) an
- b) the
- c) –
- d) a

3. He sailed from Southampton down ... English Channel.

- a) an
- b) a
- c) the
- d) –

4. Go ... immediately!

- a) in
- b) into
- c) of
- d) out

5. Do you own this lovely house or do you ... it?

- a) employ
- b) rent
- c) hire
- d) appoint

6. He is fond of ... speeches in public.

- a) make
- b) makes
- c) making
- d) doing

7. I think I know ... can help us.

- a) that
- b) what
- c) which
- d) whom

8. There is ... provocative in her behavior. She is very shy and modest.

- a) something
- b) anything
- c) everything
- d) nothing

9. The students watched the famous surgeon ... the operation and couldn't help admiring his skill.

- a) made
- b) making
- c) doing
- d) do

10. The sun ... early in this part of the world.

- a) sits
- b) is sitting
- c) has set
- d) sets

Выберите правильный вариант перевода.

1) «Invalid drive specification»

- a) неверно определённый дисковод
- б) определите дисковод правильно
- в) неверное определение дисковода

- 2) «Parameters not compatible»
 а) параметры не совместимы
 б) несовместимость параметров
 в) несовместимые параметры
- 3) «Sector size too long»
 а) размер сектора слишком длинный (большой)
 б) длина размера сектора
 в) длинный секторный размер
- 4) «Too many files open»
 а) слишком многие файлы открываются
 б) слишком много файлов открыто
 в) открытие слишком многих файлов
- 5) «Target disk is non-removable»
 а) не переносится диск, на который производится копирование
 б) перенесение диска, на который производится копирование
 в) диск, на который производится копирование, не является съёмным
- 6) «Partition selection is not bootable»
 а) не осуществляйте первоначальную загрузку из выбранной совокупности частей диска
 б) не способная к первоначальной загрузке выбранная совокупность частей диска
 в) выбранная совокупность частей диска не способна к первоначальной загрузке
- 7) «Insert source diskette»
 а) дискета, с которой осуществляется копирование, вставлена
 б) вставьте дискету, с которой осуществляется копирование
 в) копирование осуществляется со вставленной дискеты

Выберите правильный перевод слова

- 1) «Устройство»
 а) device
 б) divise
 в) divice
 г) divese
 д) dyvice
- 2) «Выводить на печать»
 а) prynd
 б) print
 в) prind
 г) printe
 д) prinde
- 3) «Время»
 а) taim
 б) taum
 в) time
 г) tyme

4) «Дата/Число»

- а) date
- б) deit
- в) deyt
- г) dete
- д) dat

5) «Файлы»

- а) faylz
- б) failz
- в) failys
- г) fails
- д) filez

6) «Подсказка»

- а) prompt
- б) promt
- в) promp
- г) proms
- д) prompte

7) «Отладка программы»

- а) debug
- б) debag
- в) dibag
- г) de bug
- д) debak

8) «Тропа»

- а) puth
- б) part
- в) pat
- г) past
- д) path

9) «Метка»

- а) lable
- б) leible
- в) leibal
- г) label
- д) labl

10) «Перерыв»

- а) pauze
- б) porse
- в) parse
- г) pause
- д) paus