Министерство науки и высшего образования
Российской Федерации

Национальный исследовательский ядерный университет «МИФИ»

А.Г. Строилова, О.Н. Овсянникова, О.Д. Агамова, Е.Г. Иванова

АНГЛИЙСКИЙ ЯЗЫК

Учебное пособие для студентов экономического направления

Москва 2019

УДК 811.111 (075)
ББК 81.2 Англ я 7
А 64

АНГЛИЙСКИЙ ЯЗЫК: учебное пособие для студентов экономического направления [Электронный ресурс] / А.Г. Строилова, О.Н. Овсянникова, О.Д. Агамова, Е.Г. Иванова. – М.: НИЯУ МИФИ, 2019. – 120 с.

Пособие предназначено для студентов НИЯУ МИФИ, изучающих дисциплину «Английский язык: разговорная практика в предметной области» для формирования языковой и коммуникативной компетенций студентов данной специальности при реализации профессиональных коммуникативных задач. Представлен материал аутентичных текстов из современных периодических изданий по темам, которые актуальны для специалистов в области экономической безопасности.

Рекомендовано как для аудиторной, так и для самостоятельной работы студентов.

Рецензенты:
доктор филологических наук, профессор Л.А. Телегин
кандидат педагогических наук, доцент О.Ю. Иванова

ISBN 978-5-7262-2587-6

CONTENTS

Предисловие

Настоящее учебное пособие предназначено для подготовки специалистов в области информационно-аналитических технологий экономической безопасности, изучающих дисциплину «Английский язык: разговорная практика в предметной области».

Цель данного пособия в соответствии с Государственным образовательным стандартом – закрепление программы, освоенной на предыдущей ступени; изучение лексико-грамматического материала, необходимого для общения в наиболее распространенных повседневных ситуациях и извлечение информации из оригинальной литературы по специальности; развитие и совершенствование навыков различных видов речевой деятельности (чтение, говорение, аудирование и письмо); овладение навыками реферирования и аннотирования научной литературы, навыками научно-технического перевода. Кроме того, большое внимание уделяется формированию умений самостоятельной работы с научно-технической литературой для реализации профессиональных коммуникативных потребностей.

В качестве одной из основных задач в неязыковом вузе остается обучение чтению. Учебное пособие направлено на развитие навыков в четырех видах чтения – изучающего, ознакомительного, поискового и просмотрового, выбор которых определяется задачей, поставленной при работе с оригинальной литературой: аутентичными общенаучными статьями, страноведческой литературой, материалами экономического и научно-популярного характера, информацией гуманитарной направленности.

При отборе текстового материала в качестве основного критерия служила информационная ценность текстов и их соответствие требованиям программы.

Важной задачей изучения иностранного языка является обучение умению излагать содержание прочитанного в сжатом виде – в форме аннотации и реферата поэтому в пособии включены задания для формирования требуемых умений и навыков. В области обучения устной речи учебное пособие готовит специалистов к осуществлению подготовленного монологического высказывания в виде сообщения, презентации и доклада, что является наиболее типичным для сферы профессионального

общения. Предпринята попытка подготовить обучающихся к участию в диалоге и полилоге (беседа или дискуссия) в области будущей профессиональной деятельности, что предполагает необходимость развития умения выражать собственное мнение, одобрение или неодобрение чужих высказываний.

Учебное пособие также содержит материал, развивающий умения и навыки письменной речи. В этом плане предусмотрены задания, формирующие умения и навыки, необходимые для заполнения различных анкет и бланков, ведения неофициальной и официальной переписки, написания тезисов докладов.

Кроме того, в пособии предусмотрен раздел, формирующий навыки самостоятельной работы с учебным материалом.

Структура учебного пособия

Учебное пособие состоит из четырех частей, организованных по тематическому принципу. Структура подачи учебного материала для всех уроков практически одинакова.

Каждый блок – тема (Unit) состоит из четырех разделов. Выделение разделов осуществляется по основным видам речевой деятельности, однако задания каждого раздела предполагают взаимосвязанное развитие умений чтения, аннотирования, реферирования, говорения и письма, что характерно для ситуаций реальной коммуникации.

Первый раздел предполагает работу над языковым материалом, который является средством реализации речевого общения. Работа с речевым материалом начинается с введения и закрепления лексического материала по теме урока. Работа над лексикой проводится на уровне слов, фраз и предложений. Завершающим этапом этой работы является текст, который демонстрирует функционирование изучаемых лексических единиц в реальных коммуникативных условиях.

Особое внимание уделяется расширению активного и пассивного словаря. В связи с этим в каждом разделе имеются упражнения на узнавание и семантизацию интернациональных слов, на овладение словообразовательными элементами.

В основу отбора грамматического материала были приняты принцип распространенности в научно-технической литературе и принцип многозначности. В соответствии с этим в активный грамматический минимум пособия были включены наиболее употребительные конструкции в текстах, которые распространяются на значительный круг лексики. Грамматический материал пособия функционально организован, т. е. все грамматические явления органически сочетаются с лексикой в коммуникативных единицах (предложениях, текстах). Таблицы и краткие пояснения к ним обеспечивают зрительную языковую наглядность.

Все изучаемые лексические единицы и грамматические конструкции закрепляются в тексте, который демонстрирует функционирование языкового материала в ситуации языкового общения. На базе ознакомительного чтения предусматривается развитие навыков аннотирования. Упражнения, предназначенные

для этого, позволяют усвоить алгоритм построения аннотации и знакомят с речевыми клише, необходимыми для ее составления.

Раздел «Самостоятельная работа» предназначен для повторения и активизации лексико-грамматического материала урока – темы и развития навыков различных видов чтения (ключевым является изучаемое) и навыков реферирования и аннотирования. Задания этого раздела можно выполнять самостоятельно в аудитории или во время подготовки к занятию.

В разделе «Writing Practice», есть задания, которые готовят обучающихся заполнять наиболее распространенные анкеты, бланки, заявки на участие в конференции, писать неофициальные и официальные деловые письма. В некоторых уроках есть тексты, цель которых заключается в активизации навыков чтения и развитие умения написания тезисов к докладу и эссе.

В разделе «Oral Practice» представлены задания на развитие умений монологической и диалогической речи и ведения дискуссии с несколькими партнерами. Тема дискуссии задается, во-первых, темой занятия и, во-вторых, текстом, который содержит ряд вопросов – проблем для обсуждения. Обучающиеся должны прочитать текст, определить круг проблем по теме и обсудить их, используя имеющиеся в разделе речевые образцы для ведения дискуссии.

Unit 1. Information security

Grammar: Tenses (Active, Passive Voices); «If clauses»; «in case clauses»; «when clauses»; Conditionals; Multifunctional words: «it», «one», «that» Degrees of comparison (adjectives) Suffixes. Prefixes Text 1. Information security Text 2. Authenticity

Wordlist

Noun	Verb	
auditing	alter	to accept the risk
authentication	deny	to be vulnerable to
authorization	depend	to deny the risk
availability	fail	to detect tempering
breach	grant	hardware failure
confidentiality	identify	malicious intent
destruction	implement	power outages
disclosure	mitigate	to prevent denial
disruption	occur	to separate duties
ensure	permit	to submit a request
encryption	prevent	top-service attack
failure	protect	system upgrades
hacker	secure	business information: confidential, private, public, sensitive;
integrity	separate	government information: secret, sensitive, restricted, unclassified, confidential, top secret
intrusion	share	
modification	submit	
privacy	validate	
protection		
recovery		
reliability		
security		
sensitivity		
tamper		
threat		

Exercise 1. Recognize familiar words.

Security, protection, confidentiality, customer, network, auditing, integrity, computer, document, message, sensitivity, access, confidential, privacy, identification, procedure, modification, unintelligibility, impregnable, liability, incompatibility, sensitivity, accessibility.

Exercise 2. Explain the difference between the following words.

1) secure, protect, defend, guard;
2) identify, recognize;
3) ensure, provide, secure, assure, insure;
4) personal, personnel;
5) use, utilize, apply, implement;
6) prevent, avert;
7) permit, allow;
8) sensitive, confidential;
9) access, assess;
10) amass, mass;
11) evolve, develop.

Exercise 3. Give Russian equivalents of the following words and the word combinations. Use dictionaries if necessary.

Disclosure, disruption, destruction, confidentiality, authenticity, tampering, clearance, encryption, assurance, availability, repudiation, threat, vulnerability, break, information protecting, information security, confidential information, security testing, information assurance, electronic data processing, sensitive information, information systems auditing, information security professionals.

Exercise 4. Match terms with the definition.

1. Authenticate	1. Any circumstance or event with the potential to adversely impact an information system through unauthorized access, destruction and disclosure, modification of data, and/or denial of service.

2. Intrusion	2. Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited.
3. Hacker	3. To verify the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to unauthorized modification in an information system or to establish the validity of a transmission.
4. Threat	4. An unauthorized user who attempts to or gains access to an information system and the data it supports.
5. Vulnerability	5. An unauthorized act of bypassing the security mechanisms of a system.

Exercise 5. Group the synonyms.

Disrupt, modify, destroy, assure, secure, keep safe, break up, facilities, execute, break, safe, occur, share, make changes, possibility, implement, vulnerability, insure, protect, take place, happen, divide with others, weakness, split, adversary, error, settlement, enemy, mistake, capability, arrangement, assets.

Exercise 6. Decide what word cannot go with the rest.

1) amass, collect, pile, disrupt;
2) ensure, assure, secure, guarantee, cure;
3) confidential, reliable, secret, hidden, unknown;
4) user, employee, customer, consumer, client;
5) repudiate, refuse, accept, deny;
6) breach, opening, breath, breaking;
7) fraught, fraud, deception, fake;
8) evaluate, assess, estimate, access;
9) decipher, reveal, decrypt, encipher;
10) superfluity, redundancy, excess, insufficient.

Exercise 7. Choose the right form of the form of the verb.

1. This notice (was altered, has been altered). 2. The control and transmission of information (have resulted, resulted) in an explosion of new telecommunications and information processing technology. 3. Security measures (are needed, need) where "vulnerabilities" of assets exist. 4. I can't go out because I (haven't finished, finished) my report on information security. 5. Information (is transported, has been transported) electronically by local area computer networks, internetted and distributed data bases, cellular radios, packet switched radios, electronic mail and a host of other techniques. 6. In the electronic age, more so than in the past, every time information (is stored, processed or communicated, was stored, processed or communicated), a potential vulnerability is created. 7. These journals (have been brought, were brought) by our friend last Monday. 8. It already subsequently (has been used, was used) in some systems. 9. At last the problem (was discussed, has been discussed). 10. Originally electronic mail (is performed, was performed) by using standard text hardcopy.

Exercise 8. Change the sentences using passive structure.

1. They protect the Hicom systems against tampering at this year's CeBIT. 2. They have denied the access to the secret documents to all. 3. Have they read any articles about cryptography? 4. The scientists have determined the distance between the sun and the earth. 5. They break up speech information into its smallest elements, i.e. separate bits.6. They have already shown three major kinds of cryptosystem in Fig.1. 7. The cryptoanalyst always knows the encoding key, but it is unable to convert it into a decoding key. 8. There are many techniques for the conversion of the original message, known as plaintext, into its encrypted form, known as ciphertext, cipher, or code. 9. During encryption the sender modifies the plaintext string by combining it with the pseudorandom sequence to produce the ciphertext. 10. They achieve protection against unauthorized interception by a process of time division multiplex and frequency dispersion.

Exercise 9. Translate the sentences from Russian into English.

1. Коды и шифры используются, чтобы защитить информацию. 2. Зашифрованные сообщения были отправлены к 6 часам вчера. 3. Не мешай! Зашифрованное сообщение сейчас отправляют.

4. Зашифрованное сообщение только что расшифровали. 5. Текст зашифрованного сообщения будет прочитан завтра. 6. Текст зашифрованного сообщения читают уже 20 минут. 7. Этот шифр будет использован в следующем сообщении. 8. Вы невнимательно прочитали статью о новых методах шифрования. 9. Обеспечение безопасности является многогранной проблемой. 10. Большое значение имеет предотвращение целенаправленного доступа к информации.

Exercise 10. Put the verb in brackets into the correct tense.

1. They already (read) a lot of books on cryptography. 2. Bob phoned Mr. Brown to find out if Mal (find out) the solution. 3. An appropriate information-theoretic model for Steganography (propose) by Cachin. 4. Soon it (maximize) the amount of hidden information (embedding rate) while preserving security against detection by unauthorized parties. 5. The term "risks" (use) for the probabilities of the vulnerabilities, which must be individually determined. 6. The system (develop) to reduce the effect of jamming last year. 7. There (be) attempts to prove in some mathematical sense the strength of algorithms, but there remains no totally satisfactory methodology. 8. Different methods for statistical steganalysis (propose) by several researchers before the improved stenographic schemes were designed. 9. Information embedding techniques for digital watermarking (design) for several years. 10. The term Cipher often (use) to mean cryptographic algorithm, cryptogram, or cryptosystem. 11. Information embedding already (investigate) in particular in the context of digital watermarking.

Exercise 11. Translate the sentences. Define functions of «it», «one», «that».

1. Regulatory assets are **those** assets for which protection may be required by regulations, laws and policy statements. 2. **One** must study a lot to become a good specialist in the field of Information security. 3. They generally define only **one** level. 4. Yesterday, I read many English articles about new ciphers, and my friend read some French **ones**. 5. We must realize **that** past approaches to information systems security are no longer adequate. 6. **It** is only the method of protecting programs so **that** unauthorized people cannot copy them. 7. Encryption is the method of encoding data so **that** unauthorized users cannot read

the data. 8. **Those** network assets include the network components, as well as the data **that** are transmitted across the networks. 9. **That** technical education in our country is excellent is known to everybody. 10 Secure system is such a system **that** cannot be accessed without authorization. 11. **It** is of great importance to prevent purposeful access to information. 12. Since **it** is difficult to transmit and store long keys, most cryptosystems have short keys. 13. A system makes **it** easier to access all varieties of data/information stored in a computer.

Exercise 12. Use the correct form of the adjective in parentheses.

1. Static passwords are the (old) and (widespread) form of user credentials. 2. The more bandwidth the target has, the (hard) it is to DDoS. 3. They generally have access to (powerful) networking resources. 4. They had the (violent) argument I had ever heard. 5. Information may be … or … (important) and very often has a monetary value. 6. Are billboards (common) in our country than in the USA? 7. Impersonation also allows a user to connect to a server using somebody else's (broad) or more restricted access permissions. 8. Many (old) operating systems, applications, and services transfer user identification information and credentials across the network in unencrypted form. 9. Mary is the (little) athletic of all the women of the group. 10. The authentication bypassing technique is (difficult) to implement for network servers – unless the server is vulnerable to some attack over the network. 11. Modern security is interpreted (wide) than in the 20th century.

Exercise 13. Put in «when» or «if».

We put «**when**» for things, which are sure to happen When all the passwords are used, the supplicant and the authentication server will generate a new list of passwords to use. We use «**if**» for things that will possibly happen If all the passwords are used, the supplicant and the authentication server will generate a new list of passwords to use.

1. … the user is prompted for authentication, the user will enter his username as usual.

2. … the attacker does not try authentication within the 60-second period after having obtained actual credentials, the chance will be lost and the attacker will need to find another passphrase.

3. However, … an attacker manages to capture a valid passphrase for a user, the attacker will have the PIN code for the user as the first four digits of the captured passphrase.

4. … the user first generates a keypair, a smart card will be used for the actual calculation.

5. … the user needs to use his private key, the smart card must be provided along with the protecting PIN code and the private key will be read from the card.

6. … a user manages to authenticate successfully and tries to access a resource, both successful and unsuccessful attempts will be monitored by the system.

Exercise 14. Put in «if» or «in case».

If *refers to a result or consequences*	**In case** *expresses a precaution*
You should phone 999 **if** there is a fire.	A user may possess an authentication identity that has been ascertained by the authentication process in case of impersonation.

1. … authorization to access a resource was successful, the user ID of the user who accessed the resource should be provided in the audit trail to allow system administrators to track access.

2. ... an attacker does not have a user name and a password or other credentials, and is not able to authenticate to a system, he may try to bypass the authentication process.

3. The attacker can therefore debug an application … authentication.

4. … an application is running locally on a computer, and an attacker has physical access to this computer, then the attacker can potentially obtain administrative privileges.

5. An attacker may be able to bypass or alter authentication mechanisms … physical access to a computer.

6. The attacker he can use a brute force attack … exhaustive search.

Exercise 15. Complete the sentences using if or should. Translate them into Russian.

If … в условных придаточных предложениях соответствует указанию на условие Ср. с русского «Если...»	**If … should = Should …**в условных придаточных предложениях соответствует указанию на условие, связанное с будущим, но вероятность события меньше. Ср. с русского «Если вдруг …»

1. … she develop an algorithm, let me know straight away.

2. You can phone me at the hotel … you need to contact me.

3. I'm going out now … anybody phone, can you take a message?

4. … he phone, can you tell him I'll phone him back later?

5. … It's impossible that you'll see her at the meeting … you see her, can you ask her to phone me?

Exercise 16. Complete the sentences. Translate them into Russian.

If you <u>ask</u> him …, Если ты попросишь его, Present simple	… he <u>will</u> do it он это сделает. Future simple

1. If I … (find) your credentials, I … (tell) you.

2. If you … (use) different methods for stegoanalysis, the improved steganographic … (design).

3. If we … (not hurry), we … (be late).

4. I must hurry. My friend … (be annoyed) if I … (not be) on time.

5. If this system… (develop), it … (reduce) the effect of jamming.

Exercise 17. Complete the sentences. Translate them into Russian.

If you asked him …, Если бы ты попросил его, Past Simple	…. he would do it. он бы это сделал. Would + инфинитив без to

1. What … you (do) if you … (create) a new algorithm?
2. If I …. (sell) my computer, I …. (not get) much money for it.
3. If you …. (take) more exercise, you …. (feel) better.
4. If I …. (not go) to the meeting, they ….. (be offended).
5. If the phone …. (ring), I … (answer) it.

Exercise 18. Translate the sentences into Russian.

If you had gone there…, Если бы вы пошли туда (вчера), if + Past Perfect	… I should have met you. я бы встретил вас. should/would + Perfect infinitive без to

1. If J. London had not learned life from his own experience, he couldn't have written his great works.
2. If I had known you were in hospital, I would have gone to visit you.
3. I would have gone out if I hadn't been so busy.
4. If I'd had a camera, I would have taken some photographs.
5. If I had been in a hurry, I would have solved the problem quicker.

Exercise 19. Translate the sentences into Russian.

Если условные (придаточные) предложения содержат глаголы «had», «were», «could», «should», то возможна бессоюзная связь главного и придаточного предложений. В этом случае эти глаголы ставятся перед подлежащим! Перевод таких предложений следует начинать с союза «если (бы)».

1. Had he a key, he could decipher the message.
2. Should he come, ask him to wait.

3. Were the surface of the bearing harder the loss of power to overcome the friction would be less.

4. Had the phones not been equipped with all the necessary instruments, it would have been difficult to maintain reliable two – way radio communication.

5. Should a man go into store-rooms for radio-active materials, the radiation would kill him.

Exercise 20. Translate the sentences into Russian.

If only

Вводит пожелание («если бы только») и может сочетаться с **would**. Однако это, как правило, не относится к глаголам, которые выражают статическое состояние (пр. like, believe, love, see и т.д.)

1. If only he would talk to me.
2. If only I knew the password.
3. If only she would come.
4. If only he would call me.
5. If only you saw this algorithm.

Exercise 21. Remember a few word groups, which can be regarded as reduced adverbial clauses.

If any – если хоть сколько-нибудь… (чего-нибудь)

If anything (anybody) – если хоть что-нибудь (кто-нибудь)

If anywhere – если хоть где-нибудь…

If at all – если данное действие происходит вообще…

If ever – если хоть когда-нибудь…

If not – если это не так…

If so – если это так…

Few, if any, little, if any – практически ничего, вообще хоть сколько-нибудь.

Exercise 22. Choose the right alternative.

1. Please, report to reception if/when you arrive at the hotel.
2. It's not cold now but take your coat with you if/in case it gets cold later.

3. We've arranged to play tennis tomorrow but we won't play if/when it's raining.

4. What would you do if/when you lost your keys.

5. You should insure your information if/in case it is stolen.

6. I'll take a bottle of water if/in case I get thirsty.

7. Can you buy me a magazine water if/in case you pass a kiosk on your way home?

8. If/when you decipher this message, you'll solve this problem.

9. When/if the post office is open, can you buy me some envelopes.

10. I'll change a travellers' cheques if/when the bank is open.

11. Such records appear, on the evidence currently available, to be held, if anywhere/if any, in the United States.

12. In case/if the response is incorrect make use of another strategy.

Reading

TEXT 1

Exercise 1. Answer the questions before reading the text

1. What is Information security?
2. Why is it very important today?
3. Why is much attention paid to information security in many countries?
4. What components do information systems include?
5. What are the differences between information security and information assurance?
6. When was the first cipher invented?

Information security

Information security components: or qualities, i.e., confidentiality, integrity and availability (CIA). Information systems are decomposed in three main portions: hardware, software and communications with the purpose to identify and apply information security industry standards, as mechanisms of protection and prevention, at three levels or layers: physical, personal and organizational. Essentially, procedures or policies are implemented to tell people (administrators, users and operators) how to use products to ensure information security within the organizations.

1. Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. The terms «information security», «computer security» and «information assurance» are incorrectly used interchangeably. These fields are often interrelated and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them. These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms. Computer security can focus on ensuring the availability and correct operation of a computer system without concern for the information stored or processed by the computer.

2. Governments, military, corporates, financial institutions, hospitals, and private businesses amass a great deal of confidential information about their employees, customers, products, research, and financial status. In modern world most of this information is collected, processed and stored on electronic computers and transmitted across networks to other computers. Should confidential information about businesses, customers or finances or a new product line fall into the hands of a competitor, such a breach of security could lead to lost business, lawsuits or even bankruptcy of the business. Protecting confidential information is a business requirement, and in many cases also an ethical and legal requirement. For the individual, information security has a

significant effect on privacy, which is viewed very differently in different cultures.

3. The field of information security has grown and evolved significantly in recent years. As a career choice there are many ways of gaining entry into the field. It offers many areas for specialization including, securing network(s) and allied infrastructure, securing applications and databases, security testing, information systems auditing, business continuity planning and digital forensics science, to name a few.

4. Since the early days of writing, heads of state and military commanders understood that it was necessary to provide some mechanism to protect the confidentiality of written correspondence and to have some means of detecting tampering.

5. Julius Caesar was credited with the invention of the Caesar cipher 50 B.C., which was created in order to prevent his secret messages from being read should a message fall into the wrong hands.

6. World War II brought about many advancements in information security and marked the beginning of the professional field of information security.

7. The end of the 20th century and early years of the 21st century saw rapid advancements in telecommunications, computing hardware and software, and data encryption. The availability of smaller, more powerful and less expensive computing equipment made electronic data processing within the reach of small business and the home user. These computers have quickly become interconnected through a network generically called the Internet or World Wide Web.

8. The rapid growth and widespread use of electronic data processing and electronic business conducted through the Internet, along with numerous occurrences of international terrorism, fueled the need for better methods of protecting the computers and the information they store, process and transmit. The academic disciplines of computer security, information security and information assurance emerged along with numerous professional organizations – all sharing the common goals of ensuring the security and reliability of information systems.

9. For over twenty years information security has held that confidentiality, integrity and availability (known as the CIA triad) as the core principles of information security.

10. Confidentiality is the property of preventing disclosure of information to unauthorized individuals or systems. For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred.

11. Breaches of confidentiality take many forms. Permitting someone to look over your shoulder at your computer screen while you have confidential data displayed on it could be a breach of confidentiality. If a laptop computer containing sensitive information about a company's employees is stolen or sold, it could result in a breach of confidentiality. Giving out confidential information over the telephone is a breach of confidentiality if the caller is not authorized to have the information. Confidentiality is necessary (but not sufficient) for maintaining the privacy of the people whose personal information a system holds.

12. In information security, integrity means that data cannot be modified without authorization. This is not the same thing as referential integrity in databases. Integrity is violated when an employee accidentally or with malicious intent deletes important data files, when a computer virus infects a computer, when an employee is able to modify his own salary in a payroll database, when an unauthorized user vandalizes a web site, when someone is able to cast a very large number of votes in an online poll, and so on.

13. There are many ways in which integrity could be violated without malicious intent. In the simplest case, a user on a system could mistype someone's address. On a larger scale, if an automated process is not written and tested correctly, bulk updates to a database could alter data in an incorrect way, leaving the integrity of the data compromised. Information security professionals are tasked with finding ways to implement controls that prevent errors of integrity.

14. For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it

must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks.

Exercise 2. Look through the text to answer the questions.

1. What is information security?
2. What is the difference between information security and computer security?
3. Why has the information security grown and evolved significantly in recent years?
4. When was the mechanism to protect information provided?
5. When did rapid advancements in information encryption begin?
6. What are the basic principles of information security?
7. What is confidentiality?
8. What is confidentiality necessary for?
9. What is integrity?
10. What does availability mean?

Exercise 3. Read the text and complete the sentences.

1. Information security means … .
2. The terms information security, computer security and information assurance share … .
3. Information security is concerned with … .
4. Computer security can focus on … .
5. The field of information security offers … .
6. Since early days of writing it was necessary to … .
7. World War II saw … .
8. The core principles of information security are … .
9. Confidentiality is … .
10. Integrity means … .

Exercise 4. Give the English for.

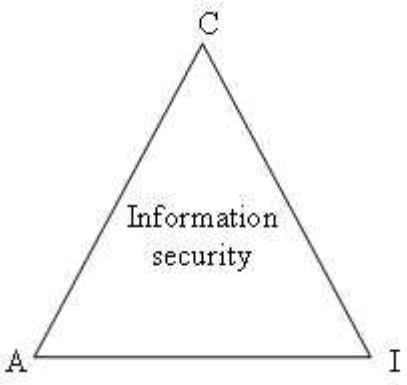
Информационная безопасность, неавторизованный доступ, раскрытие, разрушение, уничтожение, гарантирование (страхование), целостность (достоверность), доступность, накапливать информацию, конфиденциальная информация, нарушение безопасности, проверка безопасности, обнаружение

подделки, чувствительность информации, шифрование данных, обработка информации, допуск к информации ограниченного доступа, надежность информационных систем.

Exercise 5. Find and translate the paragraphs in which:

1. The term «information security» is defined.
2. The importance of information security for governments, military, business is explained.
3. The growth of significance of information security in recent years is considered.
4. The history of information security development is described.
5. The confidentiality and its breaches are outlined.
6. The definition of «integrity» is given.
7. The term «availability» is defined.
8. The aim of information systems.

Exercise 6. Describe the CIA Triad.



Exercise 7. Read the text. Make the following steps.

1. Identify the subject matter of the text.
2. Divide the text into several logical parts.
3. Identify topic sentences in each part.
4. Express the main idea of each part.
5. Define the main terms and their definitions.

Exercise 8. Read the text. Make the following steps to write the précis of the text*:*

1. Read the sentence that expresses the main idea of the text.
2. Examine each paragraph and point out the topic sentences.
3. Read the topic sentence / sentences in each paragraph.
4. Read the key words in each paragraph.

Exercise 9. Read the text and make up the summary using the following phrases.

1. Information security is one of the topic problem because … .
2. The text … considers with … .
3. It is published in … .
4. It defines the term «information security» as … .
5. It makes difference between the terms … .
6. The importance of information security for different field of … is stressed.
7. The text gives the historical survey of … .
8. Special attention is paid to … .
9. Since the text touches upon the problems of … it can be interesting to … .
10. That is why it should be recommended to … .

Exercise 10. Make sure you know the following words.

Authenticity, transaction, threat, vulnerability, countermeasure, asset, harm, impact, availability, integrity, confidentiality, assessment, productivity, protection, intrusion, privilege, separation, malicious acts.

Exercise 11. Guess the meaning of the verbs.

1) to outline	1) outline – очертание, набросок, схема, конспект;
2) to estimate	2) estimate – оценка, смета;
3) to mitigate	3) mitigation – уменьшение, смягчение;
4) to occur	4) occurrence – случай;
5) to promote	5) promotion – продвижение, повышение, содействие;
6) to adhere	6) adherence – приверженность, строгое соблюдение;
7) to submit	7) submission – подчинение, представление, подача;
8) to validate	8) validation – утверждение, ратификация.

TEXT 2

Authenticity

1. In computing, e-business and information security it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim they are.

2. **Non-repudiation**

In law, non-repudiation implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction. Electronic commerce uses technology such as digital signatures and encryption to establish authenticity and non-repudiation.

3. **Risk management**

Security is everyone's responsibility. Security awareness poster U.S. Department of Commerce / Office of Security.

A comprehensive treatment of the topic of risk management is beyond the scope of this article. We will however, provide a useful definition of risk management, outline a commonly used process for risk management, and define some basic terminology. The CISA Review Manual 2006 provides the following definition of risk management: «Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization».

4. There are two things in this definition that may need some clarification. First, the *process* of risk management is an ongoing iterative process. It must be repeated indefinitely. The business environment is constantly changing and new threats and vulnerability emerge every day. Second, the choice of countermeasures (controls) used to manage risks must strike a balance between productivity, cost, effectiveness of the countermeasure, and the value of the informational asset being protected.

5. **Risk** is the likelihood that something bad will happen that causes harm to an informational asset (or the loss of the asset). A vulnerability

is a weakness that could be used to endanger or cause harm to an informational asset. A threat is anything (manmade or act of nature) that has the potential to cause harm.

6. The likelihood that a threat will use a vulnerability to cause harm creates a risk. When a threat does use a vulnerability to inflict harm, it has an impact. In the context of information security, the impact is a loss of availability, integrity, and confidentiality, and possibly other losses (lost income, loss of life, loss of real property). It should be pointed out that it is not possible to identify all risks, nor is it possible to eliminate all risk. The remaining risk is called *residual risk.*

7. A risk assessment is carried out by a team of people who have knowledge of specific areas of the business. Membership of the team may vary over time as different parts of the business are assessed. The assessment may use a subjective qualitative analysis based on informed opinion, or where reliable dollar figures and historical information is available, the analysis may use quantitative analysis.

8. In broad terms the risk management process consists of: identification of assets and estimating their value. Include: people, buildings, hardware, software, data (electronic, print, other), supplies.

Conduct a threat assessment. Include: Acts of nature, acts of war, accidents, malicious acts originating from inside or outside the organization.

– Conduct a vulnerability assessment, and for each vulnerability, calculate the probability that it will be exploited.

– Evaluate policies, procedures, standards, training, physical security, quality control, technical security.

– Calculate the impact that each threat would have on each asset.

– Use qualitative analysis or quantitative analysis.

– Identify, select and implement appropriate controls.

– Provide a proportional response.

– Consider productivity, cost effectiveness, and value of the asset.

– Evaluate the effectiveness of the control measures.

– Ensure the controls provide the required cost effective protection without discernible loss of productivity.

9. For any given risk, Executive Management can choose to accept the risk based upon the relative low value of the asset, the relative low frequency of occurrence, and the relative low impact on the business. Or, leadership may choose to mitigate the risk by selecting and

implementing appropriate control measures to reduce the risk. In some cases, the risk can be transferred to another business by buying insurance or out-sourcing to another business. The reality of some risks may be disputed. In such cases leadership may choose to deny the risk. This is itself a potential risk.

Exercise 12. Read the text to answer the questions:

1. What is necessary in computing, e - business and information security?
2. What technology is used in electronic commerce?
3. What is risk management?
4. What is the process of risk management?
5. What is a vulnerability?
6. What is a threat?
7. Who carries out a risk management?
8. What does the risk management consist of?
9. What can Executive Management choose for a risk?

Exercise 13. Read the text without consulting the dictionary. Pencil-mark the unknown words, if any, and try to deduce their meaning relying on the context. Consult the dictionary to see if you were right.

Exercise 14. Examine Paragraph 1. Do the following:

1. Give the English equivalents to: информационная безопасность, гарантированность, сделка, подлинный, подтвердить, сторона, утверждать.
2. Identify the part of speech of the following words. State their functions in the contexts:

a – in computing …
b – … to ensure …
c – … to validate …
d – … involved …
e – … claim …

3. Express the main idea of the paragraph.

Exercise 15. Examine Paragraphs 2, 3 and answer the questions:

1. What does non - repudiation imply?

2. What technology does electronic commerce use to establish authenticity and non - repudiation?

3. What is risk management?

Exercise 16. Examine Paragraphs 2, 3 to identify the following structures. State their functions in the sentences:

1) …. to fulfill …
2) …. having received …
3) … having sent …
4)… to establish …
5) … of identifying …
6) … used …
7) … deciding …
8) … in reducing …
9) …. based …

Exercise 17. Read Paragraph 4. Make the following steps:

1. Copy out the words equivalent to: текущий, интерактивный, угроза, уязвимость, возникать, выбор, контрмеры, справляться, найти, ресурс.

2. Identify the following structures. State their functions in the sentences:

a) … ongoing …
b) … he repeated …
c) … charging …
d) … used …
e) … to manage
f) … strike …
g) … being protected …

Exercise 18. Read Paragraph 5 to answer the questions:

1. What is a risk?
2. What is a vulnerability?
3. What is a threat?

Exercise 19. Examine Paragraphs 6, 7 and give Russian equivalents of: to cause harm, to inflict harm, impact, loses, it should be pointed out, to eliminate all risk, residual risk, risk assessment, parts … are assessed.

Exercise 20. Read paragraph 8 and translate it into Russian.

Exercise 21. Examine paragraph 9 and give Russian equivalents:
to accept the risk
to mitigate the risk
to deny the risk

Exercise 22. Write the précis of the text.

Exercise 23. Make up the summary of the text using the following phrases:
1. The title of the text is …
2. It was published in …
3. Special attention is paid to …
4. ….. are discussed in detail.
5. It is pointed out that …
6. The text is of interest to …

Written Practice

Exercise 1. Read the invitation to the conference.

Dr. A.A. Ivanov 25 September 20…
Institute of Communications
St. Petersburg
Russia

Dear Dr. Ivanov,

This letter is to call your attention to the XVI-th International Conference on Information Security to be held May 11-17 20… in London, Great Britain.

In view of your active interest in this field, we would be pleased to have you as a participant in this Conference. If you are interested in attending, please forward the application form (also enclosed) to Professor A.B. Hill, Department of Information, London, University.

Attendance to this Conference is limited to approximately 100 persons. Nevertheless, if you know of anyone who has a significant

contribution to make to this Conference, please ask him to send an application form to Professor Hill.

We are planning to allow room in the programme for short presentations of very recent work warranting general discussion.

If you are aware of such developments, we would be grateful if you could bring them to the attention of the Conference Chairman.

Sincerely yours,
G.A. Phillips
Conference Secretary.

Exercise 2. Act as Ivanov. Write a letter to the Organizing Committee to say that you cannot accept the invitation.

Institute of Communications
St. Petersburg
Russia
1 October 2018

Prof. A.B. Hill
Department of Information
University of London
London
England

Dear Prof. Hill,

I am greatly honored by the … of G.A. Phillips, of September 25th inviting me to p… in the XVI-th International C… on information S…

However, I am afraid I'll have to decline your kind i…, for I have no p…of attending the C…, owing to a prior engagement for that t…

Of people whose w… I am well acquainted with, I would s… Dr. N.A. Novikov of St. Petersburg U… who will be a… to give an admirable review of the ….

I would appreciate it … if you … send me the Proceedings of the C…

Please accept my best regards,

Yours sincerely
A.A. Ivanov

Exercise 3. Write an essay «The methods of information security» (to be done at home).

The materials for your essay

TEXT 1

The Elements of Electronic Information Security

Electronic information security is composed of several disciplines and encompasses a wide range of applications and environments. These disciplines are tailored to one or more areas of protection, such as communications security or computer security. However, the general terms include:

– Cryptography: cryptography consists of the encryption and decryption processes. Encryption is the process of passing information through a mathematical process to make the information unintelligible to anyone who does not have the means (formula or algorithm and key) to decrypt the information.

– Key: in most sophisticated encryption schemes, a variable is used to periodically change the algorithm so that even if an adversary captures the encrypted information and has the algorithm they can not easily decrypt the information unless they also capture the key. Protection of the key is extremely important.

– Key distribution: the method of putting the periodic keys in the place they are needed when they are needed. This distribution may be either electronic or physical, but must be accomplished in a highly secure manner.

– Access control: the processes and systems by which the person attempting electronic access to information is validated as being the person they claim to be (authentication) and the electronic restrictions by which only authorized persons are granted access to specified information.

– Tamper protection: a series of processes, both electronic and physical, established to detect any attempts to physically intrude on electronic information or tamper with the security parameters. Protective measures taken as a result of intrusions are included in the category of tamper protection.

– Recovery: the best way to recover from a system failure is to avoid having the failure in the first place. Therefore, most security systems have built-in fail-safe features to prevent information loss or compromise from deflectable forms of failure.

TEXT 2

Security Classification for Information

An important aspect of information security and risk management is recognizing the value of information and defining appropriate procedures and protection requirements for the information. Not all information is equal and so not all information requires the same degree of protection. This requires information to be assigned a security classification.

The first step in information classification is to identify a member of senior management as the owner of the particular information to be classified. Next, develop a classification policy. The policy should describe the different classification labels, define the criteria for information to be assigned a particular label, and list the required security controls for each classification.

Some factors that influence which classification information should be assigned include how much value that information has to the organization, how old the information is and whether or not the information has become obsolete. Laws and other regulatory requirements are also important considerations when classifying information.

Common information security classification labels used by the business sector are: public, sensitive, private, confidential. Common information security classification labels used by government are: Unclassified, Sensitive But Unclassified, Restricted, Confidential, Secret, Top Secret and their non-English equivalents.

All employees in the organization, as well as business partners, must be trained on the classification schema and understand the required security controls and handling procedures for each classification. The classification a particular information asset has been assigned should be reviewed periodically to ensure the classification is still appropriate for

the information and to ensure the security controls required by the classification are in place.

TEXT 3

Access Control

Access to protected information must be restricted to people who are authorized to access the information. The computer programs, and in many cases the computers that process the information, must also be authorized. This requires that mechanisms be in place to control the access to protected information.

The sophistication of the access control mechanisms should be in parity with the value of the information being protected – the more sensitive or valuable the information the stronger the control mechanisms need to be. The foundations on which access control mechanisms are built start with identification and authentication.

Identification is an assertion of who someone is or what something is. If a person makes the statement «Hello, my name is John Doe», they are making a claim of who they are. However, their claim may or may not be true. Before John Doe can be granted access to protected information it will be necessary to verify that the person claiming to be John Doe is really John Doe.

Authentication is the act of verifying a claim of identity. When John Doe goes into a bank to make a withdrawal, he tells the bank teller he is John Doe (a claim of identity). The bank teller asks to see a photo ID, so he hands the teller his driver's license. The bank teller checks the license to make sure it has John Doe printed on it and compares the photograph on the license against the person claiming to be John Doe. If the photo and name match the person, then the teller has authenticated that John Doe is who he claimed to be.

There are three different types of information that can be used for authentication: something you know, something you have, or something you are. Examples of something you know include such things as a PIN, a password, or your mother's maiden name. Examples of something you have include a driver's license or a magnetic swipe card. Something you are refers to biometrics. Examples of biometrics include palm prints, finger prints, voice prints and retina (eye) scans. Strong authentication

requires providing information from two of the three different types of authentication information. For example, something you know plus something you have. This is called two factors authentication.

On computer systems in use today, the Username is the most common form of identification and the Password is the most common form of authentication. Usernames and passwords have served their purpose but in our modern world they are no longer adequate. Usernames and passwords are slowly being replaced with more sophisticated authentication mechanisms.

After a person, program or computer has successfully been identified and authenticated then it must be determined what informational resources they are permitted to access and what actions they will be allowed to perform (run, view, create, delete, or change). This is called authorization.

Authorization to access information and other computing services begins with administrative policies and procedures. The policies prescribe what information and computing services can be accessed, by whom, and under what conditions. The access control mechanisms are then configured to enforce these policies.

Different computing systems are equipped with different kinds of access control mechanisms – some may even offer a choice of different access control mechanisms. The access control mechanism a system offers will be based upon one of three approaches to access control or it may be derived from a combination of the three approaches.

The non-discretionary approach consolidates all access control under a centralized administration. The access to information and other resources is usually based on the individuals function (role) in the organization or the tasks the individual must perform. The discretionary approach gives the creator or owner of the information resource the ability to control access to those resources. In the Mandatory access control approach, access is granted or denied basing upon the security classification assigned to the information resource.

To be effective, policies and other security controls must be enforceable and upheld. Effective policies ensure that people are held accountable for their actions. All failed and successful authentication attempts must be logged, and all access to information must leave some type of audit trail.

TEXT 4

Cryptography

Information security uses cryptography to transform usable information into a form that renders it unusable by anyone other than an authorized user; this process is called encryption. Information that has been encrypted (rendered unusable) can be transformed back into its original usable form by an authorized user, who possesses the cryptographic key, through the process of decryption. Cryptography is used in information security to protect information from unauthorized or accidental discloser while the information is in transit (either electronically or physically) and while information is in storage.

Cryptography provides information security with other useful applications as well including improved authentication methods, message digests, digital signatures, non-repudiation, and encrypted network communications.

Cryptography can introduce security problems when it is not implemented correctly. Cryptographic solutions need to be implemented using industry accepted solutions that have undergone rigorous peer review by independent experts in cryptography. The length and strength of the encryption key is also an important consideration. A key that is weak or too short will produce weak encryption. The keys used for encryption and decryption must be protected with the same degree of rigor as any other confidential information. They must be protected from unauthorized disclosure and destruction and they must be available when needed. PKI solutions address many of the problems that surround key management.

TEXT 5

Defense in Depth

Information security must protect information throughout the life span of the information, from the initial creation of the information on through to the final disposal of the information. The information must be protected while in motion and while at rest. During its life time, information may pass through many different information processing

systems and through many different parts of information processing systems. There are many different ways the information and information systems can be threatened. To fully protect the information during its lifetime, each component of the information processing system must have its own protection mechanisms. The building up, layering on and overlapping of security measures is called defense in depth. The strength of any system is no greater than its weakest link. Using a defense in depth strategy, should one defensive measure fail there are other defensive measures in place that continue to provide protection.

Recall the earlier discussion about administrative controls, logical controls, and physical controls. The three types of controls can be used to form the basis upon which to build a defense-in-depth strategy. With this approach, defense-in-depth can be conceptualized as three distinct layers or planes laid one on top of the other. Additional insight into defense-in- depth can be gained by thinking of it as forming the layers of an onion, with data at the core of the onion, people as the outer layer of the onion, and network security, host-based security and application security forming the inner layers of the onion. Both perspectives are equally valid and each provides valuable insight into the implementation of a good defense-in-depth strategy.

TEXT 6

Using User Authentication

There are two ways of restricting access to documents: either by the hostname of the browser being used, or by asking for a username and password. The former can be used to, for example, restrict documents to use within a company. However if the people who are allowed to access the documents are widely dispersed, or the server administrator needs to be able to control access on an individual basis, it is possible to require a username and password before being allowed access to a document. This is called user authentication.

Oral Practice

Exercise 1. Take part in the discussion:
«Problem of vulnerabilities, risks and protective measures».

a) Read the text which should be taken into consideration. Think of some more.

TEXT 7

Vulnerabilities

Vulnerabilities are ascertained in many ways: first-hand experience, through the experience of others, intuition, extrapolation, or through exercises (simulated or postulated attacks). One of the main objectives of this book is to point out vulnerabilities. For now, we will mention a few general vulnerabilities associated with each of the six environments.

Physical vulnerabilities include entrances to computing areas that have insufficient protection, unreliable environmental control (air conditioning, water protection), unreliable power, and weak fire protection. Environmental and fire protection can also create hardware, software, and network vulnerabilities.

Personnel environment vulnerabilities are those that can be caused by personnel (mistakes or moral and character weakness such as greed, blackmail or bribery), and those that can happen to personnel (injury, death).

The regulatory environment vulnerabilities comprise the same personnel weaknesses mentioned above, plus those due to incomplete, contradictory or improper regulations, laws, and policy.

Hardware vulnerabilities include environmental effects on hardware, (electrical overstress, overheating, radiation), and marginal design (not allowing sufficiently for component variations, changes or failures). Unintentional emanations (TEMPEST) are also included.

Software has some of the same vulnerabilities because of the storage media used and because of other interactions between software and hardware (electrical overstress, overheating and radiation), software design can also create a vulnerability, for example, through unexpected performance in response to design errors (bugs). Its performance can also be affected by hardware component drift and by unexpected or improper user or operator actions. Another software vulnerability is failure to generate and update backup copies.

Network vulnerabilities include physical and hardware vulnerabilities as well as insufficient protection against jamming,

tapping, and other forms of interception. A vulnerability can also be created through lack of redundancy (alternate transmission routes).

Risks. We have used the term «risks» for the probabilities of the vulnerabilities, which must be individually determined (the effects of these failures in terms such as damage, losses and fines).

Protective Measures

The identification of protective measures is another important part of this book. For now, we will briefly mention a few in each category. Physical protective measures include locks, surveillance devices (alarms, closed circuit television) and environmental protection systems (fire extinguishing, power stabilization and backup systems).

Personnel protective measures include environmental control as a means of reducing the probability of injury or death and measures to protect against personnel threats (background investigation, surveillance, auditing transactions, following up on tips).

The major regulatory protective measures are to formulate comprehensive, noncontradictory, and fair regulations, laws, and policies, and then to enforce them,

Hardware protective measures include redundancy end fault-tolerant design, generous design margin allowances, and designs that take advantage of particular hardware characteristics (e.g., read-only memories to which writing is essentially impossible).

Protective measures implemented in software include access control logic such as passwords, structured development methodology for correctness and transparency and encryption.

Encryption also provides a valuable network protective measure, as do various access control schemes such as security controllers and key distribution centers.

b) Discuss the problem using the following formula of politeness.

Lack of certainty, lack of knowledge	
1. Sorry (I'm afraid), I don't know. 2. I wouldn't know. 3. I wish I knew (I had known). 4. As (so) far as I know…	К сожалению, я не знаю. Право, не знаю. К сожалению, я не знаю (не знал).

5. I've no idea. I haven't the slightest idea. 6.If I remember rightly … 7. If I am not mistaken …	Насколько мне известно. Понятия не имею. Понятия не имею. Если мне не изменяет память… Если я не ошибаюсь …
agreement	
1. I agree with you 2. I absolutely (completely, fully) agree with you. 3. I am of the same opinion. 4. That's right (true). I share your opinion. I am of the same opinion.	Я согласен с вами. Я абсолютно (полностью) согласен. Я придерживаюсь того же мнения. Правильно … Я разделяю ваше мнение. Я того же мнения.
disagreement	
1. I'm afraid you are mistaken. 2. Just the reverse. 3. I fully (completely) disagree with you.	Боюсь, вы ошибаетесь. Наоборот … Я совершенно с вами не согласен.

Exercise 2. Make up a project: «Modern Techniques in Information Security in the Modern Society».

Unit 2. Economic security

Grammar: Infinitive
Complex subject. Complex object
Text 1. The concept of economic security of the state
Text 2. The structure of economic security of the state

Exercise 1. Study the words and phrases.

Wordlist

Nouns	Verbs	Adverbs/ adjectives	Phrases
aggravation capacity competitiveness depreciation leverage load protection resistance security superiority sustainability threat(s)	complement coincide defense determine ensure imply quest withstand	adverse domestic dramatically integral intensive obvious superficial vital	adverse factors; bowels of the Earth; defence production; expanded reproduction; exchange value of currency; industrial capacity; integral part; macroeconomic indicators; on a par with; policy uncertainty; steady growth; venture capital; vital interest; wear of fixed assets; well-defined objectives.

Exercise 2. Match the nouns from the glossary with their meanings.

1. Superiority 2. Leverage 3. Sustainability 4. Resistivity 5. Aggravation 6. Depreciation	1. If someone or something aggravates a situation, they make it worse. 2. Resistance to something such as a change or a new idea is a refusal to accept it. 3. A decrease in the exchange value of currency against gold or other currencies brought about by excess supply of that currency under conditions of fluctuating exchange rates. 4. The fact that one person or thing is better, stronger, etc. than another. 5. Leverage is the ability to influence situations or people so that you can control what happens. 6. The ability to be sustained, without causing problems such as inflation.

Exercise 3. Translate the following sentences. Name part of speech of the words in bold.

1. The Australian team soon demonstrated their **superiority** over the opposition.

2. His function as a Mayor affords him the **leverage** to get things done through attending committee meetings.

3. Concerns around energy and **sustainability** are going to be with us for many years.

4. The U.S. wants big cuts in European agricultural export subsidies, but this is meeting **resistance**.

5. Stress and lack of sleep can **aggravate** the situation.

6. Dollar **depreciation** raised the cost of U.S. imports.

Exercise 4. Match the adjectives with their synonyms.

Adjectives	Synonyms
1) adverse 2) vital 3) integral 4) dramatic 5) domestic	1) lively, important, necessary 2) household, national, state, internal 3) essential, basic, fundamental, necessary 4) unfavorable, bad, threatening, hostile 5) drastic, strong, severe, harsh, extreme

Grammar

Infinitive

Exercise 1. Study grammar rules and examples.

Active		
Indefinite Infinitive (to) V1	He wants to write another letter. Он хочет написать еще одно письмо. Did you really tried to open this can. Ты правда пытался открыть эту банку?	К глаголу добавляется частица to, и вопросы будут задаваться так же, как и в русском языке: «что делать?» или «что сделать?»
Continuous Infinitive (to) + be + V(-ing)	I happened to be listening to music at very moment he came. В тот момент, как он пришел, я как раз слушал музыку. He seemed to be breathing hard. Казалось, он дышит очень тяжело.	Применяется в том случае, когда нужно показать длительность и употребляется для отображения процесса, который происходил в один и тот же отрезок времени, что и другое действие.
Perfect Infinitive to + have + V(3; -ed)	I'm glad to have invited him yesterday. Я рад, что пригласил его вчера He turned out to have left his home many years ago. Оказалось, что он покинул свой дом много лет назад.	Основное назначение – отобразить уже совершенное действие, которое произошло до какого-то момента. Не стоит путать термин Perfect Infinitive с Past Tense. Это универ-

		сальное название подходит для того, чтобы отобразить предшествующее действие, и не может быть сравнимо ни с одним из Past Tenses.
Perfect Continuous Infinitive to + have + been + V(ing)	He happened to have been waiting for me for two hours when I came. Оказалось, он ждал меня 2 часа перед тем, как я пришел. They seemed to have been working all day night. Казалось, они работали весь день.	Показывает длительное действие, которое к тому же совершалось до какого-то упомянутого момента в прошлом.
Passive		
Passive Indefinite Infinitive to be + V(3; –ed)	He wanted all the tasks to be done as soon as possible. Он хотел, чтобы все задания были сделаны как можно скорее. It is pleasant to be loved. Приятно быть любимым.	
Passive Perfect Infinitive (to) have been + V(3; -ed)	The text seemed to have been translated earlier. Оказалось, что текст перевели раньше. I found out the painting to have been stolen. Я обнаружил, что картину украли	
Complex Object		
	We noticed the woman enter the house through the back door. Мы заметили, как женщина вошла через заднюю дверь. I saw them walk along the road. Я видел, как они шли по дороге. I did not hear her say this because she spoke in a soft voice. Я не слышал, как она это сказала, потому что она говорила тихо.	**Complex object** в английском языке переводится придаточным дополнительным предложением, вводимым союзами «как», «что», «чтобы». Существительное или местоимение в этом сложном дополнении соответствует подлежащему, а инфинитив – сказуемому придаточного предложения.
Complex Subject		
	She is known to live in France. Известно, что она живет во Франции. The film festival was reported	Конструкция **Complex Subject** в английском языке применяется с определенными глаголами. Эти

	to take place in July this year. Сообщили, что кинофестиваль пройдет в июле в этом году. He was thought to study here. Думали, что он учится здесь. The car was seen to disappear. Видели, как машина скрылась. The student is expected to become a famous writer. Ожидают, что этот студент станет известным писателем. He seems to be sleeping. Кажется, что он спит.	глаголы условно можно разделить на несколько групп. Осведомленность, знание, утверждение: to know (знать), to think (думать), to state (заявлять, утверждать), to report (сообщать), to say (говорить), to announce (сообщать). Предположение: to expect (ожидать), to suppose (предполагать), to believe (верить), to consider (считать, полагать), to ask (спрашивать). Восприятие: to see (видеть), to hear (слышать), to notice (отмечать). Также Complex Subject в английском языке используется после таких словосочетаний, как to be likely (вероятно), to be unlikely (маловероятно), to be certain (несомненно), to be sure (обязательно).

Exercise 2. Define the forms of the Infinitive (Passive or Active; Indefinite, Continuous, Perfect or Perfect Continuous) in the following sentences.

1. I want to see your design. 2. It can be done. 3. The mistake must be found. 4. We knew him to be working in the room. 5. They are likely to be being served now. 6. I remember to have seen her somewhere. 7. We thought the mistake to have been found. 8. He must have been working all night. 9. She appeared to have been leading a very busy life before. 10. It’s nice to be sitting here with you. 11. It’s good to have finished work for the day. 12. I’m sorry not to have come on Friday. 13. I appear to have made a small mistake. 14. I didn’t expect to be invited. 15. There is a lot of work to do. 16. There is a lot of work to be done.

Exercise 3. Replace the subordinate clauses by infinitives in various functions.

Model: A: The child is very proud *that he pressed the button in the lift.* B: The child is very proud <u>to press</u> the button in the lift.

1. I am proud *that I have completed this work by the 1-st of June*.
2. We are glad *that we have seen this game*.
3. There is a lift in the house *which takes us to the upper stories*.
4. She said she was sorry *that she had missed you*.
5. I'm sorry *that I didn't come on Friday*.
6. We have a comfortable bed *in which you can sleep*.
7. He bought some beautiful pictures *which he will hang in his study*.
8. Ann was surprised *when she heard Peter's voice*.

Exercise 4. Begin these sentences with 'it' and put the infinitive to the end.

Model: A: <u>To make</u> mistakes is easy.

B: It is easy <u>to make</u> mistakes.

1. To explain what I meant was impossible.
2. To complete our research on time was important for the project.
3. To sell my car was difficult.
4. To get finished on time was a great feeling.

Exercise 5. Insert an active or a passive infinitive from the list below.

1. She was delighted … to the party.
2. She was delighted … her friends to the party.
3. I hate … you but I can't move the table alone.
4. She hated … with questions concerning the cost of her furniture.
5. The room … as a nursery should be warm enough.
6. His intention is … this room as a nursery.
7. She was anxious for us … her taste in decorating the flat.
8. Her taste in furnishing the room should …

(to invite, to use, to praise, to bother)

Exercise 6. Complete the following sentences using the infinitive with or without to.

1. The teacher asked us _____ (listen) to his explanations.
2. He made the students _____ (write) the composition.

3. The teacher let us _____ (use) the dictionaries.

4. The teacher noticed me _____ (open) my dictionary several times.

5. I made myself _____ (write) as neatly as I could.

6. The teacher watched us _____ (work) and didn't say anything.

Exercise 7. Open the brackets and use the Complex Object.

1. Do you want (they / stay) at the hotel?
2. I would like (the professor / look through) my report.
3. We considered (he /be) an honest person.
4. I would like (the dress / buy) by Sunday.
5. He doesn't want (they / be late) for dinner.

Exercise 8. Combine the sentences using the Complex Object.

Example: ***I felt something hard. It hurt my leg. – I felt something hard hurt my leg. I saw Mike. He was entering the house. – I saw Mike entering the house.***

1. They didn't notice us. We passed by.
2. Mike heard Sam. She was playing the violin.
3. I felt her hand. It was shaking.
4. I heard them. They were arguing.
5. We many times heard him. He told this story.

Exercise 9. Translate the following sentences. Mind the sentences with the Complex Subject.

1. He is said to know all about it. 2. He was said to have known the whole truth about it. 3. Juriy Gagarin is known to be the first man in the world to travel into space on the 12th of April, 1961. 4. He is supposed to be a very good film actor. 5. He is believed to be innocent of the crime. 6. Innocent people were announced to have been murdered by terrorists. 7. The terrorist was announced to have been killed by his own bomb. 8. The exhibition of 19th century French painting is expected to open by the end of next week. 9. Monet's painting is reported to be on exhibition until the end of the month. 10. The President of Russia was reported to speak to the nation on television tonight. 11. The American astronaut Neil Armstrong is known to be the first man to walk on the moon. 12. He was said to be one of the most promising nuclear

physicists. 13. He is said to be a good translator. 14. Roberta was known to be an honest and hard-working girl. 15. Clyde was expected to arrive at the weekend.

Exercise 10. Rewrite the following sentences using the Complex Subject.

1. People consider the climate there to be very healthy. 2. It was announced that the Chinese dancers were arriving next week. 3. It is expected that the performance will be a success. 4. It is said that the book is popular with both old and young. 5. It is believed that the poem was written by an unknown soldier. 6. It is supposed that the playwright is working at a new comedy. 7. It is reported that the flood has caused much damage to the crops. 8. It was supposed that the crops would be rich that year. 9. It has been found that this mineral water is very good for the liver. 10. Scientists consider that electricity exists throughout space. 11. It is said that the weather in Europe was exceedingly hot last summer. 12. It was reported that five ships were missing after the battle.

Exercise 11. Read the following text and mind the infinitives in various functions.

Many issues to deal with food shortage are not straightforward. Food aid has to be provided in order to fight against chronic shortages, but it needs to be carefully managed to avoid hurting local farmers. Food aid will at best provide short-term relief. Therefore, a long-term solution is to investigate ways to boost the productivity of agriculture, especially in developing countries where poverty is at its highest.

Reading

TEXT 1

Exercise 1. Try to answer the questions before reading the text.

1. What is economic security?
2. Why is it very important to achieve a high level of economic security?
3. Why do some countries desire to complement their superiority and economic leverage over other countries?

The concept of economic security of the state

In the Law of the Russian Federation «About safety» the concept of «national security» is defined as «the state of protection of vital interests of person, society and state from internal and external threats». The «vital interests» are represented as «a set of needs, the satisfaction of which reliably ensures the existence and possibility of progressive development of personality, society and state».

Thus, economic security is an integral part of national security. The economic security can be represented as the state of protection of national economy from external and internal threats, which ensures the progressive development of society, its economic and socio-political stability, despite the presence of adverse external and internal factors.

The state economic security is a complex socio-economic concept, reflecting a wide range of ever-changing conditions of material production, internal and external threats to the country's economy.

In this regard, it should also be noted that for the state there are situations when there are no external and internal threats to the national economy.

It is obvious that the economic security of a nation is determined primarily by the condition of productive forces and socio-economic relations, the extent of use of achievements of scientific and technological progress in the sector structure of foreign trade. In this regard, it can be argued that the material basis of economic security of the state are developed productive forces capable of ensuring the expanded reproduction and the civilized life of citizens. The state's economic security is closely linked with the concepts of «development» and «sustainability» of the economy.

The development of the national economy is one of the components of economic security. If the economy does not develop, the state has dramatically reduced the possibility of resistance to negative external and internal influences.

The stability of the national economy as a single system means strength and reliability of its elements, economic and organizational links between them, and the ability to withstand internal and external loads.

For example, in periods of history the USSR/Russia, characterized by high level of economic security, there was a progressive

development of the economy, coinciding with steady growth in its macroeconomic indicators.

It is obvious that the main factors of economic security of the country are: its geographical location; natural resources; industrial and agricultural potential; the degree of socio-demographic development and, finally, the quality of public leadership.

USA, Russia, Japan, China, the EU and several other countries in the world occupy a leading position in the world industrial capacity, agricultural production, natural resources, favorable geographical position, which helps to ensure their economic security.

However, they sometimes differ sharply on their industrial potential, mineral resources, socio-demographic development, as well as the nature of state regulation of the economy that largely determines the differences in the level of protection of their national economy.

(http://csef.ru/en/politica-i-geopolitica/223/ekonomicheskaya-bezopasnost-rossii-ponyatie-struktura-sravnitelnaya-i-perspektivnaya-oczenka-905)

Exercise 2. Look through the text and answer the questions.

1. What is the concept of national security?
2. How can national security be linked to economic security?
3. How can you define the concept of «state economic security»?
4. Is it common for the state to be in the situations of external and internal threats to national economy?
5. What conditions determine the economic security of a nation?
6. What is considered to be the material basis of economic security?
7. How is the state economic security linked with the concepts of development and sustainability of the economy?
8. What does progressive development of the economy coincide with?
9. What are the main factors of economic security of the country?
10. What do the countries such as USA, Russia, Japan, China, and the EU differ sharply on?

Exercise 3. Read the text and complete the sentences.

1. The concept of national security is defined as…
2. The vital interests are represented as…

3. The economic security can be represented as…
4. The state economic security reflects…
5. The economic security of a nation is determined primarily by…
6. The material basis is capable of…
7. The state's economic security is closely linked with…
8. The development of the national economy is…
9. The stability of the national economy as a single system means…
10. USA, Russia, Japan, China, the EU and several other countries in the world occupy…

Exercise 4. Give the English for the following phrases.

Жизненно важный интерес, внутренняя и внешняя угроза, неотъемлемая часть, неблагоприятные факторы, непрерывно меняющийся, способный обеспечивать расширенное воспроизводство, ресурсосбалансированность, существенно сокращать, сопротивляемость, надежность, противостоять внутренним и внешним нагрузкам, стабильный рост, макропоказатели, занимать лидирующие позиции, промышленный потенциал, благоприятное географическое положение, во многом определяет различия.

Exercise 5. Find and translate the paragraph in which:

1. The term «national security» is defined.
2. The term «economic security» is explained.
3. The economic security as an integral part of national security is considered.
4. The material basis of economic security of the state is described.
5. The stability of the national economy as a single system is outlined.
6. The example of the USSR's history in economic security is given.

Exercise 6. Read the text. Make the following steps.

1. Identify the subject matter of the text.
2. Divide the text into several logical parts.
3. Identify topic sentences in each part.
4. Express the main idea of each part.

Exercise 7. Read the text. Make the following steps to write the precis of the text.

1. Read the sentence that expresses the main idea of the text.
2. Examine each paragraph and point out the topic sentences.
3. Read the topic sentence/sentences in each paragraph.
4. Read the key words in each paragraph.

Exercise 8. Read the text and make up the summary using the following phrases.

1. The subject of the article is …
2. The article states that …
3. It was published in …
4. It defines the term «economic security» as …
5. It makes difference between the terms …
6. Some advantages are presented …
7. The text gives the historical survey of …
8. Special attention is paid to …
9. Since the text touches upon the problem of … it can be interested to …
10. That is why it should be recommended …

Exercise 9. Make sure you know the following words.

Competitiveness, knowledge-intensive, defence production, well-defined objectives, public funding, within the framework of, venture capital, technological parity, aggravation, outbreak of confrontation, domestic loan, fuel and energy complex, depreciation, capital asset, wear of fixed assets, bowels of the earth, intangible assets, economic entities.

Exercise 10. Guess the meaning of the verbs.

1) to determine –	1) determination – решимость, решительность;
2). to ensure –	2) insurance – гарантия, страховка;
3) to defend –	3) defense – оборона, защита;
4) to quest –	4) quest – поиск, разыскивание;
5) to consider –	5) consideration – рассмотрение, обсуждение;
6) to imply –	6) implication – нечто подразумеваемое, намек;
7) to announce –	7) announcement – объявление, извещение;
8) to aggravate –	8) aggravation – обострение, усиление.

Exercise 11. Read Text 2

TEXT 2

The structure of economic security of the state

Composite structural elements of economic safety of the state are: technological, techno-industrial, monetary, raw materials, energy, environmental, information and environmental components.

Technological component of economic security determines that the state is of scientific and technical potential of the country, which ensures the competitiveness of national goods and services in the markets of knowledge-intensive (high-tech) products, but also ensures self-development in shortest possible time the latest technological solutions that define the leading breakthroughs in the civil industries and defence production.

World practice shows that the technological component of economic security is only possible if the national economy is on the path of innovative development. An effective innovation system is characterized by a well-defined objectives on a national scale for innovative development of national economy; large in comparison with other countries spending on research and development (R & d) on creation of innovative technologies; public funding of a significant portion of these costs; protection of intellectual property within the framework of state innovation policy (promoting active patenting); the close connection between innovative companies and universities; a large share of venture capital in total R & d funding.

Of great importance for the economic security of the state is its ***technical component***. It is understood as the ability of the national economy to compensate quickly in case of violation of foreign economic relations, or internal socio-economic shocks for their negative consequences, and steadily to carry out expanded reproduction, to meet the public (including defense) needs. It is closely connected with logistical and social factors of production.

Dependency on foreign supplies is a particular threat to national security. Such dependence can lead to significant economic difficulties and even loss of economic independence in case of economic aggravation, or the outbreak of a direct military confrontation.

Monetary component can be defined as the ability of the state to get, to place and use domestic and foreign loans and investments, and to ensure sustainable functioning of its monetary system as well as the satisfaction of public needs in unfavorable external and internal economic conditions.

World experience shows that the sustainability of economic growth and economic security of the state is possible only in case of investment development of national economy. Each country has its own implementation of this type:

* the investments are expected to be 20 to 25 % of GDP (capitalization);

* the share of foreign direct investment should be not less than 15 – 17 % of the internal volume;

* the degree of wear of fixed assets should not exceed 30 – 35 %.

Food **and** ***raw materials*** involve the security of the country's economy in the sizes required for the effective functioning of the national economy. The most important measure to ensure food and raw material component of the economic security of the United States, Canada and other postindustrial countries is the financial support of the agriculture from the state budget, support and lobbying of agricultural exports. Provision of essential commodities is also one of the main factors of economic security of the state. Thus, the problem of ensuring food and resource security is the dependence of national economy on imports of food and raw materials.

The energy component of the economic security of the state implies the physical stability of energy supplies for domestic consumption and the ability of national economy to adapt to the new world prices.

One of the main problematic issues here is the creation of a diversified structure of energy imports and energy resources as well as introduction of energy saving technologies.

Other problems involve depreciation of capital assets, the gap of domestic and world energy prices, the pace and scale of nationalization and privatization in industry, the growth of accidents at the enterprises of fuel and energy complex of the country.

The environmental component involves the state of the national economy, which is aimed to prevent or timely resolve contradictions between society and the environment. The solution to the problem of environmental pollution is closely linked to the restriction of human

activities and primarily with neutralization of anthropogenic impacts on natural ecological systems, the ozone layer of the atmosphere, the earth, its bowels, superficial and underground waters, atmospheric air, forests and other vegetation, fauna, microorganisms, genetic Fund and natural landscapes.

The information component involves the guaranteed reliable mutual exchange of industrial, scientific-technical and other information within the business complex of the state and foreign partners.

Exercise 12. Answer the questions:

1. What are the composite structural elements of economic safety of the state?
2. What does technological component of economic security ensure?
3. What is the main function of the technical component of economic security?
4. What significant economic difficulties can occur in case of economic aggravation?
5. How can monetary component be defined?
6. What is the problem of ensuring food and resource security?
7. What issues does the energy component involve?
8. What is the environmental component aimed to prevent?
9. Why is the information component important?

Exercise 13. Read the text without consulting the dictionary. Pencil-mark the unknown words, if any, and try to deduce their meaning relying on the context. Consult the dictionary to see if you were right.

Exercise 14. Examine paragraph 1 and do the following:

1) Give the English equivalents to the following words: технологический компонент, потенциал страны, конкурентоспособность, достижение в производстве продукции оборонного назначения.

2) Now build the logical sentence using the English equivalents of the given above words and the following verbs: *to determine, to ensure, to lead to.*

3) Examine paragraph 1, 2 and express the main idea of the paragraphs.

Exercise 15. Do the following:

1) Finish the sentences:

Technical component is understood as the ability to compensate ...

Technical component is understood as the ability to carry out ...

Technical component is understood as the ability to meet ...

2) Now examine paragraph 3 and check your sentences.

3) Rephrase the sentence. Use the following words:

economic, aggravation, outbreak, military, confrontation, dependence, foreign, supply, lead, loss, economic independence.

4) Examine paragraph 4 and check your sentence.

Exercise 16. Examine paragraph 5 to identify the following structures. State their functions in the sentences:

1) … can be defined …
2) … to get, to place, to use
3) … ensuring …
4) … are expected to be …
5) … should be not …
6) … should not exceed …

Exercise 17. Rephrase the sentences and say what two main factors determine food and raw material component.

– To ensure, food and raw material component, financial support, agriculture, state budget, lobbying, agricultural exports.

– Provision, essential commodities, economic security, the state.

Exercise 18. Examine paragraph 8, rephrase the sentences and check your answer.

Exercise 19. Speak about the main problematic issues of the energy component of the economic security. Use phrases below to help you.

Creation, diversified structure, energy imports, energy resources, introduction, energy saving technologies, depreciation, capital assets, domestic prices, world energy prices, nationalization, privatization, industry, accidents, energy complex.

Exercise 20. Examine paragraph 9, express the main idea of the paragraph and check your answer.

Exercise 21. Examine paragraph 10, express the main idea of the paragraph and rephrase the sentences:

1) … to prevent …
2) … to resolve …
3) … to neutralize …

Exercise 22. Write the precis of the text.

Exercise 23. Make up the summary of the text using the following phrases:

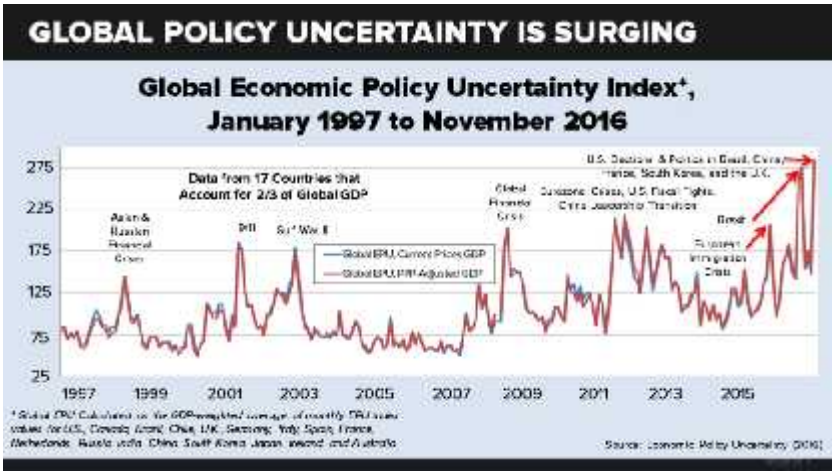
1. The title of the text is …
2. Special attention is paid to …
3. … are discussed in detail.
4. It is pointed out that …
5. The text is of interest to …

Written Practice

Exercise 1. a) Match Russian words and phrases with their English equivalents:

1) неясность мирового экономического курса 2) показатель 3) колебание 4) паритет покупательной силы 5) регулирование покупательской способности 6) валовый внутренний продукт 7) фискальные разбирательства	1) purchasing power adjustment amount 2) fiscal fights 3) gross domestic product (GDP) 4) global economic policy uncertainty 5) index 6) purchasing power parity (PPP) 7) surging

b) Now examine the chart below.



Exercise 2. Summarize the information by selecting and reporting the main features, and make comparison where relevant. Write at least 150 words. Use the following samples of descriptions.

Samples of Descriptions

1) Skeleton plan

The graph shows /pictures /visualizes /represents /tracks the progress /evolution /dynamics /sequence of…

It gives indication of…

The annual revenue of the (company) is sorted by product division/industries/gender (or any other category)

In… (spending) assumes an upward trend…/tends upwards/ moves up the graph

In… (…) assumes a negative trend/tends downwards/moves down the graph

The year of… is marked by…

The increase is represented by a moderate/modest rise…

Continued to decrease by (%, number or volume) on (time period)

The most affected areas/spheres/industries are…

For the second/third/ fourth consecutive year…

….kept growing in (year or month) with a substantial increase of…(%, number or volume) over (year or month)

All together it amounts to/ accounts for… (%, number or volume)
The supply outruns/outplays/offsets the demand
To (sky) rocket/sore vs to plummet/drop dramatically
To recover by… to…
To level off at (level, index)

Exercise 3. Write an essay «Real economic crisis – Food» (to be done at home). The materials for your essay:

TEXT 1

Why Food Prices Have Increased?

Whilst the West worries over rising petrol prices and the scarcity of mortgages, the developing world faces a threat to the most basic necessity of life-enough food to eat. After decades of abundant food supplies, recent years have seen a marked increase in the price of food. In the west, this just about reaches our attention as we note the price of bread passes £1. But, for those living on $1 – $2 a day or less, the increased food prices can be devastating, leaving many below the poverty line.

Why Food Prices Have Increased?

Increasing Demand has come from:

1. Economic growth in China and India. Increased living standards mean people are consuming more food and also more land intensive foods. For example, as incomes rise people buy more meat. Meat is more land intensive, because you need both land for the livestock and also crops to feed the livestock.

2. Growing Population. The world's population is currently 6.5 billion this is forecast to grow up to 9 billion in a couple of decades.

3. Demand for Biofuels. As the west look for alternatives to oil, governments are encouraging the use of biofuels which are supposed to provide an environmentally friendly alternative to oil. However, the increased demand is pushing up prices.

Problems with Supply.

1. Environmental problems. Global warming is contributing to desertification of former arable areas. Therefore, some countries are experiencing declines in available agricultural areas. In western

countries, it has proved difficult to increase productivity of arable land. Increased use of fertilisers e.t.c has reached a point of diminishing returns.

2. Inelastic Supply. Another problem related to agriculture is the time lags involved in growing crops. Most crops can only be grown once a year. It can take even longer to prepare land for more crops. Therefore, the high prices have not been able to encourage more supply; eventually the high prices may encourage more supply, but, by then it may be too late contributing to the volatility of food prices.

3. Restrictions facing Local Farmers. In many developing countries agriculture is characterised by small scale farmers, who lack the ability to invest in new technology and enable more efficient farming. Basically, despite the rise in prices, there is little that many farmers can do to increase supply.

How To Deal with the Food Shortages?

To deal with food shortages is not straightforward. There are many issues to consider. In the short term aid is necessary to deal with chronic shortages. But, at the same time, food aid needs to be carefully managed to avoid hurting local farmers. Aid will at best provide short term relief. A long term solution is to investigate ways to boost the productivity of agriculture, especially in developing countries where poverty is at its highest. Food shortages and price increases spark violence and debate.

TEXT 2

Global food crisis

by Mark Hughes

The 2008 food crisis, which has seen dramatic increases in food prices and food shortages and has sparked riots and political turmoil in a number of countries, took the world by surprise. While the debate centers on identifying the causes and finding solutions, the effects have already been all too clear and are continuing to mount.

Effects of the 2008 Food Crisis

Prices for basic foods such as rice, wheat, and corn have risen 83 % since 2005. Compared to the first half of 2007, food prices in 2008 rose even more dramatically: 130 % increase for wheat and an 87 % increase for soy. Between March 3rd and April 23rd, 2008, the price for a metric ton of rice rose from $460 to $1,000. This almost doubling in price

caused riots in Egypt and Haiti. Other nations (Cameroon, Ivory Coast, Mauritania, Ethiopia, Uzbekistan, Yemen, the Philippines, Thailand, Indonesia, and Italy) have experienced violent protests in reaction to the increased cost of food staples.

During the summer months, twenty-nine countries have cut back on food exports to ensure their populations have enough to eat. India, Vietnam, China, and more have limited or banned exports of rice. Pakistan and Bolivia have severely capped wheat exports. Kazakhstan has even restricted exporting sunflower seeds.

Causes of the Food Crisis

Increased demand on the food supply has caused the price of food to rise. The numerous contributors to the rise in cost and the reduction in supply include biofuels, bad weather, the historically high cost of oil and transportation, increased demand for meat and dairy, and population growth.

Biofuels

Plant material, or biomass, is used to produce biofuels in the form of gas or liquid fuel. Energy and environmental concerns have helped promote biofuels as a way to replace oil and natural gas. Unfortunately, biofuels seem to be exacerbating the problem of food shortage. Farmers in many industrialized nations, such as the United States, have been encouraged by their governments to switch to growing fuel crops, such as corn and soy. This reduction in domestic farming means food must be imported, which increases the overall cost of food production worldwide.

Natural Forces

Drought in Australia

Australia is normally the second largest exporter of grain, after the U.S. The continent, though, is experiencing an ongoing drought that has been described as the worst in a century. Grain yields have shrunk and many silos remain empty. Australia's drought is a major factor in global wheat stocks being at their lowest since 1979. In fact, many wheat and rice farmers are switching to crops that demand less water, such as wine grapes.

Desertification

In 2008, 110 countries on every continent (excluding Antarctica) are experiencing widespread drought and desertification. Imagine the

fertile, moist soil on a farm turning into the dry, blowing sand of a desert, which is what the term desertification is describing. It happens when the soil has been ruined and can no longer support life.

Overgrazing by farm and herd animals confined by fences is a big contributor to desertification. Fencing restricts the amount of land available for animals to graze, which in turn prevents the soil and plants from recovering after being trod upon and eaten. Deforestation, slash-and-burn agriculture, and the use of trees and plants as fuel have also contributed to the increasing spread of desertification, especially in semi-arid and arid regions.

Oil and Transportation

The price of a barrel of oil exceeded $100 in 2008. Oil provides the energy needed for farmers to plant and harvest their crops. The more money it costs to grow an ear of corn translates into an increase in the cost to sell it. For instance, energy is needed to produce fertilizer, keep equipment like tractors running, and provide the fuel to transport the finished crops all over the world. Many industrialized nations no longer produce enough of their own food, which means food must be imported from elsewhere. The increase in oil and fuel prices has made the transport of food prohibitively expensive for some nations.

Meat and Dairy

Economic growth in many countries has allowed people to expand their diets, especially in China and other Southeast Asian nations. More and more people have been adding meat and dairy to the menu. Cows must eat more grain in order to supply enough meat and milk to meet demand. For instance, 700 calories of animal feed must be consumed in order to produce a 100-calorie piece of beef.

Population Growth

The human population has grown significantly in the first decade of the 21st century. As of April 2008, the global population reached 6.6 billion people, up from 6 billion in 1999. The increase in the number of people means greater competition for resources.

What is being done?

There is no simple answer to the causes of the food crisis. Biofuels are getting a lot of attention, due in part to the newness of the technology, the use of food as fuel, and whether the march toward switching energy resources over to biofuels is intensifying, if not causing, the food crisis. Rich nations are being asked to reconsider

many recently passed laws and policies that promote biofuels as an alternate energy source. The United Nations is also urging rich countries to increase the amount of money they give to poorer nations for food aid. In April 2008, President Bush ordered $200 million in emergency food aid to be made available to «meet unanticipated food aid needs in Africa and elsewhere». The World Bank intends to increase its agricultural lending to Africa in 2009 to $800 million.

The United Nations Secretary General Ban Ki-moon announced the establishment of a task force to handle the global food crisis. One of the priorities of this task force is to close the funding gap for the UN's World Food Program (WFP) this year. By May 1st, the size of the funding gap had reached $755 million. Mr. Ban also addressed the importance of helping farmers in poor countries who have been hurt by the increasing costs of fertilizer and energy. $200 million is being made available to help farmers in the worst affected areas to boost food production, as well as $1.7 billion is going to help nations in need buy seeds.

Robert Zoellick, the head of the World Bank, worries about nations using export bans to protect their food stocks, expressing that such controls «encourage hoarding, drive up prices, and hurt the poorest people around the world». In March India banned the export of non-basmati rice, and in late April decided to tax exports of basmati rice.

26 million Latin Americans are in danger of being pushed into extreme poverty, according to the Inter-American Development Bank. The bank has implemented a $500 million credit line to increase the amount of support to help agricultural productivity and anti-poverty programs. The Mexican government has also pledged to help offset increased food costs by increasing cash subsidies to its poorest citizens.

Oral Practice

Exercise 1. Read the information below.

Every month, millions of Americans face an impossible choice: pay for energy to power their homes, or pay for basic needs like food and medicine. TED Fellow DeAndrea Salvador is working to reduce energy costs so that no one has to make this kind of decision. In this quick talk, (script taken from Ted Talks web site), she shares her plan to help low-

income families reduce their bills while also building a cleaner, more sustainable and more affordable energy future for us all.

De Andrea Salvador's speech

So, as a child, I used to spend all of my time at my great-grandmother's house. On hot, humid, summer days, I would dash across the floor and stick my face in front of her only air conditioner. But I didn't realize that that simple experience, though brief, was a privileged one in our community. Growing up, stories of next-door neighbors having to set up fake energy accounts or having to steal energy seemed normal to me. During the winter, struggling to get warm, my neighbors would have no choice but to bypass the meter after their heat was shut off, just to keep their family comfortable for one more day. These kinds of dangerous incidents can take root when people are faced with impossible choices.

In the US, the average American spends three percent of their income on energy. In contrast, low-income and rural populations can spend 20, even 30 percent of their income on energy. In 2015, this caused over 25 million people to skip meals to provide power to their homes. This is when energy becomes a burden. But energy burdens are so much more than just a number. They present impossible and perilous choices: Do you take your child to get her flu medicine, or do you feed her? Or do you keep her warm? It's an impossible choice, and nearly every month, seven million people choose between medicine and energy.

This exposes a much larger and systemic issue. Families with high energy burdens are disproportionately people of color, who spend more per square foot than their white counterparts. But it's also nurses, veterans and even schoolteachers who fall into the mass of 37 million people a year who are unable to afford energy for their most basic needs. As a result, those with high energy burdens have a greater likelihood of conditions like heart disease and asthma.

Look-given our rockets to Mars and our pocket-sized AI, we have the tools to address these systemic inequities. The technology is here. Cost of renewables, insulation, microgrids and smart home technology are all decreasing. However, even as we approach cost parity, the majority of those who own solar earn much more than the average

American. This is why, when I was 22, I founded the nonprofit RETI. Our mission is to alleviate energy burdens by working with communities, utilities and government agencies alike to provide equitable access to clean energy, energy efficiency and energy technology.

But there's no one way to solve this. I believe in the power of local communities, in the transforming effect of relationships. So we start by working directly with the communities that have the highest energy burdens. We host workshops and events for communities to learn about energy poverty, and how making even small updates to their homes like better insulation for windows and water heaters can go a long way to maximize efficiency. We're connecting neighborhoods to community solar and spearheading community-led smart home research and installation programs to help families bring down their energy bills. We're even working directly with elected officials, advocating for more equitable pricing, because to see this vision of energy equity and resilience succeed, we have to work together sustainably.

Now, the US spends over three billion a year on energy bill payment assistance. And these programs do help millions of people, but they're only able to help a fraction of those in need. In fact, there is a 47-billion-dollar home-energy affordability gap, so assistance alone is not sustainable. But by building energy equity and resilience into our communities, we can assure fair and impartial access to energy that is clean, reliable and affordable. At scale, microgrid technology, clean technology and energy efficiency dramatically improve public health. And for those with high energy burdens, it can help them reclaim 20 percent of their income – 20 percent of a person's income who's struggling to make ends meet. This is life-changing. This is an opportunity for families to use their energy savings to sponsor their future.

I think back to my great-grandmother and her neighbors, the impossible choices that they had to make and the effect it had on our whole community. But this is not just about them. There are millions nationwide having to make the same impossible choices today. And I know high energy burdens are a tremendous barrier to overcome, but through relationships with communities and technology, we have the paths to overcome them. And when we do, we will all be more resilient.

Exercise 2. a) Write general and special questions to the text above. (15 – 20 questions).

b) Take part in the discussion: "How we can make energy more affordable for low-income families". Use the following expressions for agreeing and disagreeing:

Expressing agreement

- I agree with you 100 percent.
- I couldn't agree with you more.
- That's so true.
- That's for sure.
- (slang) Tell me about it!
- You're absolutely right.
- Absolutely.
- That's exactly how I feel.
- Exactly.
- I'm afraid I agree with James.
- I have to side with Dad on this one.
- No doubt about it.
- (agree with negative statement) Me neither.
- (weak) I suppose so. I guess so.
- You have a point there.
- I was just going to say that.

Expressing disagreement

- I don't think so.
- (strong) No way.
- I'm afraid I disagree.
- (strong) I totally disagree.
- I beg to differ.
- (strong) I'd say the exact opposite.
- Not necessarily.
- That's not always true.
- That's not always the case.
- No, I'm not so sure about that.

Interruptions

- Can I add something here?
- Is it okay if I jump in for a second?
- If I might add something...
- Can I throw my two cents in?

- Sorry to interrupt, but...
- (after accidentally interrupting someone) Sorry, go ahead. OR Sorry, you were saying...
- (after being interrupted) You didn't let me finish.

Settling an argument

- Let's just move on, shall we?
- Let's drop it.
- I think we're going to have to agree to disagree.
- (sarcastic) Whatever you say. If you say so.

Unit 3. Money Laundering

Grammar: Gerund, Infinitive, Participle I, Participle II, Participial constructions Abbreviation Text 1. Money laundering in the UK Text 2. Money laundering offences

Wordlist

Verb	Adjective	
to alert to amend to identify to misuse to mitigate to undertake	cash-intensive competent movable	to act on behalf of …; the Bank Secrecy Act (BSA); applicable BSA requirements; to combat crime; to conduct an assessment; CDD (Customer Due Diligence); depository institution; Designated Non-Financial Business and Profession (DNFBP); Designated Non-Financial Business and Profession (DNFBP); enforcement mechanism; to encourage vigilance; executive order; follow-up mechanism; to keep up to date; mutual evaluation; RBA (Risk-Based Approach); PEP (politically exposed person); to raise an issue; regulatory system; SRB (Self-regulatory body); suspicious transaction reporting (STR); suspicious activity; suspicious operation; wire transfer.

Exercise 1. **Explain the meaning of the words you recognized.**

Alert, cash, financial, currency, jurisdiction, to undertake, treasure, property, authorities, measure, assessment, transaction, legal, suspicious.

Exercise 2. Explain the difference between the following words.

1) criminal, immoral, illegitimate;
2) finance, investment, banking;
3) money, capital, fund;
4) protection, insurance, care;
5) guidance, advice, instruction;
6) progress, evolution, development;
7) enhance, enlarge, increase.
8) regulation, management, control;
9) obligation, duty, requirement;
10) scrutinize, explore, inspect.

Exercise 3. Give Russian equivalents of the following words and the word combinations.

Money laundering, to conceal money, criminal activity, to invest, international policy, to tackle (money laundering), financial action, level of compliance, an instrumental role, associated regional bodies, issues of concern, strong legislation, to prevent the use of …, to set global standards on smth., a founding member, to review industry guidance, to appoint supervisors, to monitor the sector, to improve the transparency and accountability, to ensure compliance with the regulations, to implement the regulations in practice, to undertake, enhanced due diligence on smth., individuals and entities, to put policies and procedures in place, to impose penalties, national authorities.

Exercise 4. Match the word with its definition.

1	evaluate	a	a group of people doing military or police work
2	contribution	b	to think carefully about something before making a judgment about its value, importance, or quality

3	policy	c	someone who is in charge of an activity, a place, or a group of people
4	a force	d	something that you do that helps to achieve something or to make it successful
5	supervisor	e	a set of plans or actions agreed on by a government, political party, business, or other group of people

Exercise 5. Group the synonyms.

Monitoring, juridical, apprehensive, payment, measure, doubtful, legal, money, lawful, capital, suspicious, audit, mistrustful, check, cautious, legislation, authorized, regulation, act, ruling, fund, control.

Exercise 6. Find the odd one out.

1. Development, increase, achievement.
2. Conformity, coincidence, compliance.
3. Scrutinize, economize, analyze.
4. Legislation, code, law.
5. Treasure, money, cash.

Exercise 7. Choose the right form.

Gerund

Герундий – это неличная форма глагола, образующаяся путем добавления суффикса **-ing** к глаголу. Например: *read – read**ing***. Обладает свойствами глагола и существительного. В предложении может выполнять различные функции: подлежащее, именная часть составного сказуемого, дополнение, определение, обстоятельство.

Forms of the Gerund	**Active**	**Passive**
Non-perfect	taking	being taken
Perfect	having taken	having been taken

Exercise 8. Change the sentences using the Gerund.

It's impossible to tell/ to know = There's no telling/knowing
It's certain (that) = there's no denying/escaping/mistaking

It's no good (use) … , There's no/I can't see any point in … , What's the good (use) of…? What's the point in (of) …?

1. It is impossible to tell what legal base will be held here.
2. It's certain what measures were undertaken.
3. It's certain that our department won't be able to complete these orders without extra staff.
4. It's certain that this has been a difficult year for the company.
5. Your help only complicated the case.
6. It's certain that this will be a serious blow to the shareholders.
7. The share rate is very unpredictable so it is impossible to know how the market will react to the news.
8. It's barely possible for her to earn enough to support herself these days.
9. The company has reputation for a low pay and bad conditions.
10. The manager is tired of telling the staff off.

Exercise 9. Translate the sentences from Russian into English.

1. Нет смысла поднимать этот вопрос.
2. Изучив все обстоятельства дела, он внес изменения.
3. Они изменили стоимость, проведя оценку.
4. Он обычно пользуется банковским переводом.
5. Рабочие угрожали начать забастовку.
6. Я устал делать вам замечания.
7. Какой смысл читать эту статью? Информация устарела.
8. Он гордился тем, что его избрали в совет директоров.
9. Терпеть не могу разговаривать в таком тоне.
10. Личность клиента необходимо подтвердить.

Exercise 10. Study the table. Choose the correct non-finite form of the verb.

only Gerund is used after:	**only Infinitive is used after:**
to be afraid of, to be aware of, to be (in)capable of, to be conscious of, to be fond of, to be proud of, to be sure of, to be angry at	arrange, attempt, decide, expect, hope, pretend, promise, refuse, offer
admit, avoid, deny, enjoy, insist on, mind, suggest	

Verb	Meaning with the Gerund	Meaning with the Infinitive
Stop	«Перестать делать что-то».	«Для того, чтобы» (прекратить делать одно действие, чтобы сделать другое).
Regret	Сожалеть о содеянном.	Сожалеть о том, что предстоит сказать, сделать.

1. Does the agenda need (amend)?
2. The nicest thing about the mechanism is that it doesn't need (follow-up).
3. Tomas stopped (smoke) and felt much healthier.
4. Don't hesitate (call) us if you need help or a good piece of advice.
5. The manager insisted on (come) on time.
6. Whenever we met, she avoided (look) at me.
7. I don't see why we should postpone (talk) it out.
8. The BBC suggested (televise) the coronation, but the Prime Minister said no.
9. He claims (see) the accident.
10. (Be) honest, there is little chance of the scheme (approve).

Exercise 11. Translate the sentences. Explain the use of the Complex Object/Complex Subject.

	Образование	Употребление
Complex Object	Первая часть – существительное или местоимение в объектном(!)падеже, вторая часть – инфинитив/причастие настоящего времени.	После глаголов, выражающих: 1) желания, чувства; 2) предположение; 3) физическое восприятие.

Complex Subject	Первая часть – существительное или местоимение в Именительном падеже, вторая часть – инфинитив. Части разделены сказуемым.	Если сказуемое выражено глаголами в страдательном залоге или главная часть – безличное предложение

1. Jane saw the information keeping up to date.
2. I watched a customer entering the room.
3. We observed a PEP debate.
4. He felt his voice tremble.
5. I'd like this company to pay the bill.
6. His work is considered to be finished in some hours.
7. These reforms are believed to be difficult to carry out.
8. Mr. Jason was known to have been appointed to the post.
9. The documents are reported to have been received.
10. He made them go away.

Exercise 12. Translate the sentences from Russian into English using the Complex Object/Subject.

1. Компетентные органы заставили организацию проверить отчет.
2. Считают, что это честная сделка.
3. Позвольте дать Вам совет.
4. Никто не ждал, что эта работа будет закончена вовремя.
5. Мы знаем, что он очень хороший сотрудник.
6. Вы бы хотели, чтобы мы пришли на это совещание?
7. Я хочу, чтобы Вы сохранили эти сведения в тайне.
8. Используемое оборудование позволяет снизить риски.
9. Они наблюдали, как мы встретили делегацию.
10. Ожидалось, что они заплатят в иностранной валюте.
11. Сообщили, что бухгалтерский отчет принят без замечаний.

Exercise 13. What do these abbreviations stand for?

FATF, SRB, BSA, DNFBP, PEP, CDD, STR

Exercise 14. Complete the sentences with the right form of the Gerund.

1. No (walk) on the grass.
2. I like (invite) to the parties.
3. I insist on (treat) with a certain consideration.
4. She is proud of (be) so pretty.
5. Bennet was ashamed of (show) even the slightest irritation.
6. Excuse my (not answer) you before.
7. He did not remember (be) in that room.
8. (Not know) her address, he could not write to her.
9. He regretted now (come).
10 He denies (speak) to her.

Exercise 15. Study the example. Translate the sentences from Russian into English.

Абсолютная причастная конструкция (Prepositional Absolute Construction with Participle II) вводится предлогом *with*. Именная часть чаще всего выражена существительным. В предложении служит обстоятельством.

На русский язык переводится деепричастным оборотом или придаточным предложением.

*It is unhealthy to sleep with the windows **shut**.*

*He can't walk with his leg **broken**.*

1. Сотрудники сидели молча, с выключенными телефонами.
2. Они продолжали свою преступную деятельность, глава фирмы действовал от лица акционеров.
3. Мужчины стояли рядом, делать им было нечего.
4. Он не посмел бы уйти домой, если бы работа не была закончена.
5. Он сидел неподвижно, закрыв глаза руками.
6. Операционист не могла установить личность клиента при неработающем сканере.
7. С сильно бьющимся сердцем он распечатал конверт.
8. Он не мог ничего сделать, его руки связаны.
9. Адвокат отказывался приезжать без подписанного контракта.
10. Наконец-то он не боялся банкротства, получив денежный перевод.

Exercise 16. Study the example. Read the sentences. Find the Nominative Absolute Construction. Translate them into Russian.

Независимый причастный оборот (the Nominative Absolute Participial Construction) представляет собой сочетание существительного в общем падеже или местоимения в именительном падеже, причем существительное или местоимение не является подлежащим в предложении. В конструкции может использоваться как причастие I, так и причастие II. На русский язык чаще всего переводится придаточным предложением или деепричастным оборотом.

This duty completed, he had three months' leave. – ***Когда эта работа была закончена***, он получил трехмесячный отпуск.

One morning he stood in front of the tank, ***his nose almost pressed to the glass***. – Однажды утром он стоял перед витриной, ***почти прижавшись носом к стеклу***.

1. The door and the window of the vacant room being open, we looked in.
2. It being now pretty late, we went upstairs.
3. Weather permitting, we shall start tomorrow.
4. Force failing, no further hope of conciliation is left.
5. A knock had come to the door, and there being nobody else to answer it, Clare went out.
6. I can't work with the noise coming from the street.
7. I lay idly in a big chair with my eyes closed.
8. She got up, the clothes folded over her arm.
9. They walked in the cold night, fresh snow crunching noisily underfoot.
10. I wouldn't dare go home without the job finished.

Reading

Exercise 1. Answer the questions before reading the text.

1. What have you heard of money laundering?
2. What can be done to prevent it?
3. Can international regulations help solve the problems of money laundering?

TEXT 1

Money laundering in the UK

1. Money laundering is used by criminals to conceal money made through criminal activity. As a global financial centre the UK is often seen as an attractive destination for criminals to invest the proceeds of their crime.

2. The Treasury leads the UK's contribution to international policy development on anti-money laundering and terrorist finance.

The Financial Action Task Force (FATF) is the leading inter-governmental body that sets global standards on tackling money laundering and terrorist finance. The UK is a founding member of the FATF and played an instrumental role in its development.

3. Today, the FATF is made up of 34 member countries, all of which are evaluated against the 40 recommendations and nine special recommendations to establish their level of compliance and identify areas where improvement is needed.

4. Together with a network of associated regional bodies, the member countries meet regularly to review progress being made and address issues of concern.

5. We are working with the European Commission to ensure that cross-European legislation is strong enough to prevent the use of the financial system for money laundering. We have:

- published a response to the Third European Money Laundering Directive in June 2012
- helped shape proposals for a Fourth Money Laundering Directive, which are currently being scrutinised by the European Parliament and Council.

6. HM Treasury and the Home Office co-chair the Money Laundering Advisory Committee, which advises the government on its approach to preventing money laundering in the UK. Members include representatives from law enforcement, government, industry and regulators. The committee reviews industry guidance before it is approved by the Treasury.

7. The Treasury appoints supervisors to monitor the anti-money laundering and counter terrorist finance sector. In order to improve the transparency and accountability of supervision and to encourage good

practice, the Treasury has worked with supervisors to develop an annual report on anti-money laundering and counter terrorist finance supervision.

8. The first annual report on anti-money laundering and counter terrorist finance supervision was published in November 2011.

9. There are a number of industry and government bodies responsible for providing advice to businesses and ensuring compliance with the regulations. The Treasury approves guidance written by industry to help businesses understand how they should implement the regulations in practice. Courts must take into account whether an individual followed approved guidance notes when making decisions in relation to suspected money laundering.

10. HM Treasury also issues Advisory Notices regarding the risks posed by unsatisfactory money laundering and terrorist financing controls in a number of jurisdictions. Under the Counter Terrorism Act 2008, firms are required to undertake enhanced due diligence on transactions involving individuals and entities from those jurisdictions.

11. The Money Laundering Regulations 2007 require firms to put policies and procedures in place in order to prevent money laundering and terrorist financing.

12. Part 7 of the Proceeds of Crime Act 2002 creates the money laundering offences in the UK and requires the making of suspicious activity reports to the Serious Organised Crime Agency.

13. Transfer of Funds (Information on the Payer) Regulations to enforce regulation 1781/2006/EC set out by the European Parliament and Council, which imposes obligations on payment service providers when they make or receive a transfer of funds.

14. Control of Cash (Penalties) regulations, under section 2(2) of the European Communities Act 1972 allows countries to work together and share information on large-scale movements of cash in or out of the European Union. The regulations also give national authorities the power to take appropriate actions, or to impose penalties.

Exercise 2. Look through the text to answer the questions:

1. Who is money laundering used by?

2. Which is one of the attractive destinations for criminals to invest the proceeds of their crime?

3. What is the FATF?

4. How many members is the FATF made up of?

5. Who establishes the level of compliance in the member countries?

6. What prevents the use of the financial system for money laundering?

7. Which organization advises the government on its approach to preventing money laundering in the UK?

8. What is the Treasury annual report about?

9. Do industry and government take part in working out the regulations? How?

10. What regulations give national authorities the power to take appropriate actions or to impose penalties?

Exercise 3. Read the text and complete the sentences.

1. Money laundering means …

2. The terms «money laundering», «criminal activity», «government regulator» share … .

3. Money laundering is concerned with … .

4. The FATF focuses on … .

5. The FATF sets … .

6. Cross-European legislation is strong enough to… .

7. A number of industry and government bodies is responsible for….

8. The core principles of the Money Laundering Regulations are … .

9. Control of Cash (Penalties) regulations allows … .

10. The FATF member countries meet regularly to… .

Exercise 4. Give the English equivalents for the following phrases.

Отмывание денег, мировой финансовый центр, совершать преступления, вклад в международную политику, лидирующая международная организация, устанавливать международные стандарты, затрагивающий финансовые интересы террористов, представители правоохранительных органов, финансовый контроль, следить за состоянием финансового сектора, финансовая прозрачность и отчетность, ежегодный отчет, соответствие требованиям законодательства, выполнять требования, частные и юридические лица, государственные власти, вводить в действие (применять закон), налагать штрафы.

Exercise 5. Find and translate the paragraphs in which.

1. The term «money laundering» is defined.
2. The importance of anti-money laundering and terrorist finance is explained.
3. The definition of The FATF is given.
4. The history of strengthening European legislation is described.
5. The scheme of supervision of the anti-money laundering sector is considered.

Exercise 6. Describe the reason of creating the FATF.

Exercise 7. Read the text. Make the following steps.

1. Identify the subject matter of the text.
2. Divide the text into several logical parts.
3. Identify topic sentences in each part.
4. Express the main idea of each part.

Exercise 8. Read the text. Make the following steps to write the précis of the text.

1. Read the sentence that expresses the main idea of the text.
2. Examine each paragraph and point out the topic sentences.
3. Read the topic sentence/sentences in each paragraph.
4. Read the key words in each paragraph.

Exercise 9. Read the text and make up the summary using the following phrases.

1. Money laundering is the topic problem because …
2. The text … considers with …
3. It is published in …
4. It defines the term «money laundering» as …
5. It makes difference between the terms …
6. The importance of anti-money laundering and counter terrorist finance supervision for different fields of … is stressed.
7. The text gives the historical survey of …
8. Since the text touches upon the problems of … it can be interesting to …
9. That is why it should be recommended to …

Exercise 10. Make sure you know the following words.

Activity, destination, criminal, government, authorities, treasury, approach, enforcement, diligence, unsatisfactory, guidance, payment, providence, transaction, entity, regulation, impose, enhance, jurisdiction.

Exercise 11. Guess the meaning of the verbs.

1	invest	a	to believe that something is bad or worse than it appears
2	monitor	b	to introduce something (e.g. new) and force people to accept it
3	establish	c	to use your money with the goal of making a profit from it
4	suspect	d	to make something start to exist or start to happen
5	impose	e	to regularly check something or watch someone in order to find out what is happening

TEXT 2

Money laundering offences

What, then, is money laundering? Organized crime generates cash. As crime has become increasingly globalized (such as the Internet crime and people trafficking) and large scale, so revenue generated from it has increased. Where this revenue is in the form of cash, which in the case of organized crime it largely is, the cash has to be disguised and blended into the banking system. Without this happening, it would be easy for the authorities to track down the money and, therefore, the criminals. The ultimate aim of the money launderer is to get the «dirty money» into the banking system in a legitimate form, so that there can be no question that he or she came by the money in a legal way. Once the cash has moved into the banking system, it is passed into many other areas, in an attempt to cover its tracks. These different areas might include other accounts, companies which have been set up to «front» the

activity, which has generated the cash, foreign currencies and so on. Then, in turn, cash from these different sources is passed into legitimate companies and bank accounts, from which the criminals can extract the cash as apparently legitimate profit. The «dirty money» has been laundered, and is now, in all appearance, clean.

The three stages to money laundering, then, are «placement», whereby the dirty money is put into the banking system, followed by what is called «layering», in which the cash passes into many different areas in order to confuse its origins, and finally, «integration», where the cash passes into legitimate companies and accounts.

Money laundering in the UK is a criminal offence, and as such, any person involved in any known or suspected money laundering activity risks a criminal conviction carrying a jail term of up to 14 years. It is significant that even innocent involvement on the part of professionals such as bankers and lawyers can provoke a criminal charge.

There are various money laundering offences within the jurisdiction of the United Kingdom to be found in statutes such as the Criminal Justice Act 1988 (as amended), and the Terrorism Act 2000 (as amended). The main change made by these two significant pieces of legislation is that they create two new obligations to make Suspicious Transaction Reports. The legislation, then, increases the onus on professionals dealing with financial transactions of any kind to be vigilant in detecting suspicious transactions, and to act effectively upon them when such transactions do arise. When this occurs, the Suspicious Transaction Reports (abbreviated to STR) can be made either to the law enforcement authorities or, where applicable, to the nominated Money Laundering Reporting Officer.

In most professional outfits dealing with financial transactions, and particularly law firms, will have a MLRO, to whom reports should be made. This officer will have ultimate responsibility within the particular practice (be it a banking, law, or accountancy practice) to regulate the transactions of the firm. It is also this officer, however, with whom responsibility ultimately lies if a suspicious transaction passes without notice, and later turns out to have been a laundering scheme.

The first of these obligations arising in the above statutes is for an individual to make a STR if he or she suspects that either he or his organisation is about to become involved in money laundering. An example of this within the world of solicitors would be if a solicitor,

upon being instructed by a (usually new) client, suspected he was being asked to put funds into his client's account in order to conceal the funds' criminal origin. In such a situation, he would be obliged to complete a STR. As well as this, he would be obliged to get the consent of the relevant authorities before completing the transaction. Failure to do this (even if it is simply a forgetful omission) will render the solicitor guilty of a money laundering offence.

A further offence is introduced in the Drug Trafficking Act 1994 and the Terrorism Act 2000 is the offence of «failure to report». This occurs where the person knows or suspects that another person is engaged in laundering, the proceeds of drug trafficking or terrorism, and fails to make a report to the law enforcement agencies. In the case of the Terrorism Act 2000, this offence is widened to include those who had reasonable grounds for knowing or suspecting.

These statutory offences have increased the range of money laundering offences within the UK legislation, and have similarly increased the requisite degree of vigilance on the part of financial professionals. By increasing the offence to cover those who knew of another's involvement, or even had grounds for such a belief, it is no longer adequate for the financial professional to be careful in the work he alone conducts; he or she must also keep an eye on co-workers.

Exercise 12. Read the text without consulting the dictionary. Pencil-mark the unknown words, if any, and try to deduce their meaning relying on the context. Consult the dictionary to see if you were right.

Exercise 13. Read the text to answer the questions.

1. Where does large scale of revenue in the form of cash come from?
2. Why is it important to blend the cash into the banking system?
3. How can the activity, which has generated the cash, be hidden?
4. What are the three stages to money laundering?
5. What is the punishment to a person suspected money laundering activity?
6. What was changed in the legislation concerning STR?
7. Who should a STR be made to?
8. Whom does responsibility lie if a suspicious transaction passes without notice?

9. What is the first obligation for an individual to make a STR?

10. What is «the offence of failure to report»?

11. What has increased the range of money laundering offences within the UK legislation?

Exercise 14. Examine paragraph 1.

1. Give the English equivalents to the following phrases.

Организованная преступность, доходы растут, законным образом, внести в банковскую систему, различные счета, учредить фирму, скрыть происхождение (денег), иностранные валюты, «грязные/чистые» деньги, получить наличные деньги.

2. Identify the part of speech of the following words. State their functions in the contexts:

a – … organized …

b – … to generate …

c – … to include …

d – … increasingly …

e – … legitimate …

3. Express the main idea of the paragraphs.

Exercise 15. Examine paragraph 2, 3 and answer the questions.

1. At what stage is the dirty money put into the banking system?

2. How can one confuse the origin of the cash?

3. What new obligations were created in 1998-2000?

Exercise 16. Examine paragraph 2, 3 to identify the following structures. State their functions in the sentences.

1. ….to pass into …

2. ….followed by …

3. … is put into …

4. … to be found …

5. … laundering …

6. … dealing with …

7. … in detecting …

8. … abbreviated to …

9. …. be it …

10. … (turns out) to have been …

Exercise 17. Read paragraph 4. Make the following steps.

1. Copy out the words equivalent to:

возникающий в связи с…, вовлечен в отмывание денег, в кругу адвокатов, несмотря на (будучи), скрыть средства, преступного происхождения, обязан сообщить, подозрительная операция.

2. Identify the following structures. State their functions in the sentences:

a) … arising in …
b) … to become involved …
c) … upon being instructed by …
d) … was being asked …
e) … in order to conceal …
f) … the consent (of) …
g) … before completing …

Exercise 18. Read paragraph 5 to answer the questions.

1. What is a law enforcement?
2. What is a statutory offence?
3. What is the requisite degree of vigilance?

Exercise 19. Examine paragraphs 4, 5 and give Russian equivalents of the following phrases.

Arising in the above statutes, is about to become, to put funds into his client's account, conceal the criminal origin, complete the transaction, a forgetful omission, render smb. guilty, is engaged in drug trafficking or terrorism, reasonable grounds, conduct the work, keep an eye on co-workers.

Exercise 20. Read paragraph 1, pay attention to terms and translate it into Russian.

Exercise 21. Examine paragraphs 2, 3, give Russian equivalents and explain the meaning of the following phrases:

to increase the onus
the responsibility
to provoke a criminal charge

Exercise 22. Write the précis of the text.

Exercise 23. Make up the summary of the text using the following phrases.

1. The title of the text is …
2. It was published in …
3. Special attention is paid to …
4. ….. are discussed in detail.
5. It is pointed out that …
6. The text is of interest to …

Written Practice

Exercise 1. Read the example of meeting minutes.

Meeting Minutes
Good Company Inc.
Board meeting date: 11/27/2018
Meeting was called to order at 15.00. Quorum was established.

Present were:	Bob Leader, President
	Jim Writer, Secretary
	Conny Candue, Vice President
	Betsy Spender, Treasurer
	M. Johanson, Company Attorney
	Riley Reliable, Company Manager
Absent:	Norton Noshow, junior manager, excused

Reports:

- Treasure report given by Betsy Spender.
- Manager report given by Riley Reliable.
- Collections report given by M. Johanson.

Business:

- Motion: Hire R.P. Polas to complete the annual report.

Vote: Motion disapproved (one – in favour, two opposed, one abstaining).

- Motion: Accept Lovely Discovery Company written proposal to maintain the Company common property.

Vote: Motion approved (three in favour, one opposed). Discussion of recognition that Lovely Discovery was the highest bidder, but the consensus is that a good history with Lovely Discovery justifies renewing the contract.

Resolved: That Good Company Inc. accept Lovely Discovery Company written proposal to maintain the Company common property.

Meeting adjourned at 17.30.

Exercise 2. Act as Bob Leader.

a) Write a letter to Lovely Discovery to say that you accept their proposal:

256, Finnit st.
New Orlean

3520 Piedmont rd,
Atlanta GA, 30305
11/28/2018

Dear Mr. Legard,

Yours sincerely.

b) Write an essay «Legislative methods of crime combating» (to be done at home).

The materials for your essay

TEXT 1

When the new Labour Government took office in May 1997, the regulation of financial services within the United Kingdom was complex and less efficient than it should have been. Within three years of taking office, however, the wide reaching Financial Services and Markets Act 2000 had been introduced. As well as simplifying and streamlining the regulatory framework, this Act introduced the Financial Services Authority, the body charged with overseeing this regulation. A major aspect of the simplified system has been an increasing focus on the combating of money laundering. All professional persons are responsible for detecting, and alerting the appropriate authorities to such activity, but there is, perhaps, a larger degree of responsibility on solicitors than other professionals to be alert to the dangers.

Before discussing the legislative arrangements in the United Kingdom in particular relation to money laundering, it is necessary to outline the wider changes in financial regulation that have occurred since 1997. At that time, there existed a rather complex web of bodies, each answerable to another, with ultimate responsibility resting with HM Treasury. The second tier of responsibility was divided between the Bank of England (before it gained independence, obviously), the

Insurance Division, the Securities and Investments Division, and the Building Societies Commission. These, in turn, regulated further tiers of bodies, and the whole system was underpinned by five ombudsmen, a personal insurance arbitration service, and two different complaints services. Within this tangled structure, it is easy to see how money laundering could have been a problem, with so called 'dirty money' being moved around with no clear responsibility lying anywhere. The 2000 legislation, however, simplified this structure so that now, although nominal responsibility still rests with the Treasury, it is almost wholly delegated to the powerful Financial Services Authority with almost exclusive control and responsibility for financial services regulation. There are, now, just two branches under the FSA; the Financial Services and Markets Compensation Scheme, and the Financial Services Ombudsman. This streamlining has made regulation easier and more efficient purely by simplifying what was previously a haphazard and uncertain system.

TEXT 2

The main defence to a money laundering offence, however, is one which also encourages vigilance and action on the part of the professionals within financial service industries. This is the defence of reporting an offence, or a suspected offence; or even an intention to disclose, so long as this is accompanied by a reasonable excuse as to why the disclosure was not actually made. This does not include wilfully shutting one's eyes to the true situation, and there will be a rigorous standard of proof required if this defence is pleaded. The significance of both of these defences is that they both have a positive effect on the overall combating of money laundering. Although an adjunct to the legislative provisions, these defences provide great encouragement for those involved in financial services to take all steps possible to ensure no offences are being committed.

The body charged with policing the financial world in relation to money laundering is the National Intelligence Gathering Service. With the mission statement: «To provide leadership and excellence in criminal intelligence to combat serious and organised crime», one of its key functions is to combat money laundering. It is through this body (either from their website or otherwise) that one can make a Suspicious

Transaction Report. As an indication of the extent of money laundering activity, but also perhaps as a reassuring sign of the NCIS' work, in 2003, the NCIS received over 100,000 disclosures (according to their website). This constituted an increase of 60 % on the number in 2002, and almost double that of 2001. Again, rather than showing necessarily that money laundering is on the rise (although it may be), these figures reflect the success of the current legislative and regulatory arrangements within the UK in combating money laundering. As at March 2004, an estimated £25 million had been protected (that is, restrained, seized, or returned to victims) as a result of consent decisions. the NCIS works in partnership with sister agencies such as the Serious Fraud Office, the Egmont Group of Financial Intelligence Units, and the Financial Services Authority. The umbrella organisation is the Joint Money Laundering Steering Group.

With regard to the Financial Services Authority, section 6 of the Financial Services and Markets Act 2000 requires that body to aim at reducing the extent to which regulated persons and unauthorised businesses can be used for a purpose connected with financial crime. This is one of the FSA's four core aims, or statutory objectives (the other three being to protect consumers, market confidence, and public awareness). In January 2001, having recently been established by the Financial Services and Markets Act 2000, the FSA published their Policy Statement. Later that year, in July 2001, the FSA published a document entitled The Money Laundering Theme: Tackling Our New Responsibilities. These set out the objectives of the FSA in relation to money laundering specifically, as well as financial crime more generally. These included making crime more costly for criminals, achieving an industry perception of money well spent, raising consumer awareness of financial crime issues, contributing to a wider UK fight against crime, and to have a «balanced, joined up» approach to anti-money laundering and fraud.

TEXT 3

Various pieces of legislation have been consolidated by the Proceeds of Crime Act 2002. The law relating to money laundering is, then, to be found in one piece of legislation as opposed to three or four. As well as consolidating the offences discussed above, this Act extends one of the

offences considerably. This offence if the Drug Trafficking Act offence of failure to report another's involvement in laundering. Firstly, it widens the offence to bring it into line with the offence in the Terrorism Act 2000, namely that the person is under an obligation to make a STR if he or she has reasonable grounds for suspecting another's involvement. Secondly, the requirement to make a STR now extends to financial transactions involving money originating from any crime, as opposed to only drug trafficking proceeds. The failure to report offence is, however, limited in one respect. It is limited to people who come across money laundering in the course of conducting business in the «Regulated Sector». The 'Regulated Sector', as defined in Schedule 6 of the Act, is basically every institution which is obliged to comply with the Money Laundering Regulations. It is significant that despite the fact the Proceeds of Crime Act 2002 replaces the money laundering offences found in the Criminal Justice Act and the Drug Trafficking Act, the Terrorism Act 2000 continues to regulate the laundering of money related to terrorist activities.

The Proceeds of Crime Act 2002, then, criminalises anything to do with money laundering. The offences fall within Part 7 of the Act, particularly sections 327 – 342. It is here that the new offence of failure to report laundering based on reasonable grounds for suspicion is to be found. Section 340 defines the relevant terms. «Criminal property» is defined as anything which constitutes or represents a benefit from a crime (any crime as opposed to the specific ones mentioned in the earlier legislation). It goes on to define «criminal conduct» as anything that constitutes a criminal offence in the United Kingdom, regardless of where the «offence» was committed. These are clearly very wide definitions. This is necessary in order to counter the internationalization of organised crime.

An example of this is the problem of so-called «Spanish bull fighting». This is where a person has made profits from an activity which is legal within the jurisdiction that the profit was made, but then comes to the UK, where the same activity is illegal. The broad definitions of POCA catch the proceeds from such an activity for the purposes of money laundering regulation. With regard to the 'criminal property', the Act, again because of its broad definitions, covers many types of person and activity, for example, tax advisors and mortgage fraud.

Section 327 of POCA deals with the offence of «fencing». This, broadly, includes any dealings with the criminal property throughout its trail. Section 328 deals with arrangements which facilitate money laundering.

Another significant effect of these pieces of legislation is that they criminalise «tipping off» (section 333 of POCA). This is in order to prevent people warning those about whom they have made a STR. Broadly, the offence prohibits a person who suspects or knows that a STR has been made to the law enforcement authorities, to make any disclosure which might prejudice any forthcoming investigation. The starkest example of this would be informing a person that he is the subject of a STR in order to give that person time to cover his tracks and, possibly, destroy the evidence. Linked to this is the offence of prejudicing an investigation into money laundering, which is covered by section 342.

Solicitors' practices are very attractive to potential money launderers. This is because they have certain qualities which make the laundering process, if successful, virtually untraceable. Solicitors are often targeted, then, because they regularly deal with clients' money. High value transactions occur through the solicitors' books every day, and as the proceeds of organised crime are often very high indeed, transactions of a similar value help to conceal the laundering from standing out. Secondly, the practice of solicitors is heavily regulated, both from within the profession (the Law Society) and also from without. While this may appear to be an argument against using solicitors as part of the laundering process, from the point of view of the launderers, if the process is successful, there will be absolutely no suspicion remaining about the origin of the funds. Coupled with this is the supposed integrity of solicitors. Again, the practical effect of this from the point of view of the launderers, is that once the funds are extracted from the solicitors' account, there will be no question as to the money's legitimacy. Finally, solicitors are easily accessible to members of the public, so potential launderers have no problem in contacting them. In response to this increasing need for vigilance, solicitors (as well as other financial professionals) are increasingly being trained (and are increasingly required to be trained by legislation) to be alert. Causes for concern in this context include unusual settlement requests from a client. That is to say in a situation where a case might be progressing well, and the client

requests a settlement abruptly and immediately, suspicions may be aroused. Similarly, any unusual instruction from a client, particularly is they are a new client, and use of a client account, would generate suspicion.

TEXT 4

A financial institution must report any transaction that requires reporting under the terms of 31 CFR Chapter X if the transaction is conducted or attempted by, at, or through the financial institution and involves or aggregates at least $5,000 ($2,000 for money services businesses, except as provided in Section 6 of this document) and the financial institution knows, suspects, or has reason to suspect that the transaction or pattern of transactions of which the transaction is a part:

Involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity (including, without limitation, the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate or evade any Federal law or regulation or to avoid any transaction reporting requirement under Federal law or regulation;

Is designed, whether through structuring or other means, to evade any requirement of 31 CFR Chapter X or any other regulation promulgated under the Bank Secrecy Act, Public Law 91 – 508, as amended, codified at 12 U.S.C 1829b, 12 U.S.C. 1951 – 1959, and 31 U.S.C. 5311 – 5332;

Has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the financial institution knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction, or

Involves the use of the financial institution to facilitate criminal activity.

In addition to the above requirements, a bank must file a FinCEN SAR for activity involving: insider abuse involving any amount. Whenever the bank detects any known or suspected Federal criminal violations, or pattern of criminal violations, committed or attempted against the financial institution or involving a transaction or transactions conducted through the financial institution, where the bank believes that it was either an actual or potential victim of a criminal violation, or

series of criminal violations, or that the bank was used to facilitate a criminal transaction, and the bank has a substantial basis for identifying one of its directors, officers, employees, agents or other institution-affiliated parties as having committed or aided in the commission of a criminal act regardless of the amount involved in the violation.

Violations aggregating $5,000 or more where a suspect can be identified. Whenever the bank detects any known or suspected Federal criminal violation, or pattern of criminal violations, committed or attempted against the bank or involving a transaction or transactions conducted through the bank and involving or aggregating $5,000 or more in funds or other assets, where the bank believes that it was either an actual or potential victim of a criminal violation, or series of criminal violations, or that the bank was used to facilitate a criminal transaction, and the bank has a substantial basis for identifying a possible suspect or group of suspects. If it is determined prior to filing this report that the identified suspect or group of suspects has used an “alias,” then information regarding the true identity of the suspect or group of suspects, as well as alias identifiers, such as drivers’ licenses or social security numbers, addresses and telephone numbers, must be reported.

Violations aggregating $25,000 or more regardless of a potential suspect. Whenever the bank detects any known or suspected Federal criminal violation, or pattern of criminal violations, committed or attempted against the bank or involving a transaction or transactions conducted through the bank and involving or aggregating $25,000 or more in funds or other assets, where the bank believes that it was either an actual or potential victim of a criminal violation, or series of criminal violations, or that the bank was used to facilitate a criminal transaction, even though there is no substantial basis for identifying a possible suspect or group of suspects.

TEXT 5

Confidentiality of SARs:

A FinCEN Suspicious Activity Report (FinCEN SAR), and any information that would reveal the existence of the FinCEN SAR (collectively, «SAR information»), are confidential, and may not be disclosed except as specified in 31 U.S.C. 5318 (g) (2) and in FinCEN’s regulations (31 CFR Chapter X).

SAR Sharing:

FinCEN has concluded that a depository institution that has filed a SAR may share the SAR, or any information that would reveal the existence of the SAR, with an affiliate, as defined in FinCEN Guidance FIN-2010-G006 issued January 3, 2011, provided the affiliate is subject to a SAR regulation. The sharing of SARs with such affiliates facilitates the identification of suspicious transactions taking place through the depository institution's affiliates that are subject to a SAR rule. Therefore, such sharing within the depository institution's corporate organizational structure is consistent with the purposes of Title II of the BSA.

Prohibition on Disclosures by Financial Institutions:

Federal law (31 U.S.C. 5318 (g) (2)) provides that a financial institution, and its directors, officers, employees, and agents who, pursuant to any statutory or regulatory authority or on a voluntary basis, report suspicious transactions to the government, may not notify any person involved in the transaction that the transaction has been reported. Provided that no person involved in the suspicious activity is notified, 31 CFR Chapter X clarifies that the following activity does not constitute a prohibited disclosure.

TEXT 6

Finally, it is possible that money laundering offences could come within the remit of the Serious Fraud Office. This is an independent government department which investigates and prosecutes serious and complex fraud in order to maintain confidence in the probity of business and financial services within the UK. This department focuses only on serious and complex fraud, and therefore does not respond to every referred case of suspected fraud. In order for a money laundering offence to come within its remit, several factors must be met. Firstly, the value of the alleged fraud must exceed £1 million. Amounts smaller than this will not be considered sufficiently serious for the SFO to investigate. Secondly, there must be a significant international dimension to the fraud. In many modern money laundering instances, this will be the case. This is a natural effect of the fact that so much of the organised crime which generates the «dirty money» needing to be laundered is international in character. Thirdly, the case must be likely

to be of widespread public concern. Often money laundering cases will not meet this criteria, as they will only involve a closed, relatively small group of people. Occasionally, however, this will not be the case. Fourthly, the case must require specialised knowledge of financial markets. Given that many money laundering cases occur through highly complex financial trails, it is likely that this requirement will be met.

Oral Practice

Exercise 1. Take part in the discussion. «Safeguards against suspicious transactions»

a) Read the text which should be taken into consideration. Think of some more.

TEXT 7

When the Money Laundering Regulations 2003 come into force, they will substantially increase the level of regulation which financial service providers are subject to. As a general rule, the higher the level of risk that a particular activity carries, the higher the degree of regulation it will be subject to. The MLR say staff within the relevant businesses must be properly trained to be alert to potential money laundering activities. This applies to all staff, including secretaries and other support staff. 'relevant businesses' will involve, for example, those concerned with insolvency work, tax advice, financial and real property transactions (such as acting as a client's receiver), and company and trust work.

The Regulations are organised into five parts. The first part is entitled «General», and deals briefly with citation, commencement, and interpretation. This part simply states that the Regulations came into force at various points throughout 2004, and early 2005. An important definition found in Part 1 is that of what a 'relevant business' is. It is defined as a broad range of activities concerned with financial services, for example, regulated activities such as accepting deposits or managing investments, estate agency work, operating a casino, the provision of accountancy services and so on. Any dealer in high value goods will generally find themselves to be caught by the Regulations. A wide range of businesses has, then, been brought into the regulated sector, including

certain jewelers or car dealers. Often it will be the case that these businesses, uncertain of how they will be affected, will have to seek legal advice to understand the implications of the new legislation for their particular business.

Part 2 is entitled «Obligations on those who carry on relevant business». this part makes provision for systems and training to be instigated to combat money laundering, and procedures for identification checking, record keeping, and internal reporting. Part 3 is entitled «Money Service Operators and High Value Dealers», and is sub-divided into «Registration», «Powers of the commissioners», «Penalties, review and appeals», and «Miscellaneous». Part 4 is the Miscellaneous section, covering such issues as the relevant supervisory authorities, prohibitions in relation to certain countries, and so on.

One of the major changes, which these regulations have, is to widen the scope of the 'regulated' sector. This means that more professionals and industries or practices fall within the scope of the statutory provisions for combating money laundering. Similarly, the obligations upon those who count as 'regulated' persons, or engaged in regulated activities, are increased. A major area where this is the case is that of checking a client's identity. This is a significant factor as it provides a powerful means of combating potential money laundering. By checking a client's background sufficiently, a practitioner will be able to establish that the client is legitimate, and that the instruction is itself legitimate. The likely effect of this will be, potentially, a more cumbersome process of screening by professionals prior to accepting instruction. Many professionals may be unhappy about this as it prolongs the length of time before that professional can accept the instruction, and therefore get paid. There is also the issue of wanting to avoid embarrassing or upsetting the client, especially if he or she is new to the practice, by investigating whether they are genuine. There are, however, provisions for discrete investigation so as to avoid this potential embarrassment, and the overall likely effect is that fewer dubious new clients will be accepted professionals in the financial services sector.

Another significant change, which has come about as a result of the Regulations, is the altered Suspicious Transaction Report form, which is issued by the NCIS. A new form has been introduced which deals specifically with circumstances where the information being reported is

likely to be of limited intelligence value (the Limited Intelligence Value report).

Finally, the Regulations introduced a further hurdle for professionals to overcome when dealing with financial transactions which may involve money laundering. Under the new rules, consent may be necessary from the NCIS before a transaction can be carried out. From the day after this consent is sought, the NCIS have a seven working day notice period in which to issue or withhold consent. The likely effect of this provision is, again, that the procedure for completing instructions from clients will be more onerous and drawn out. This is likely to annoy professionals who will be keen to work as swiftly and efficiently for their clients as possible (in order to obtain payment, and hopefully further instructions). It means, however, that there is a further safeguard against suspicious transactions which may involve money laundering occurring.

b) Discuss the problem using the following formula of politeness:

Being (not so)certain	
1. Sorry (I'm afraid), I don't know.	К сожалению, я не знаю.
2. I'm quite certain about this	Я вполне в этом уверен.
3. I wish I knew (I had known).	Право, не знаю. К сожалению, я не знаю.
4. As (so) far as I know…	Насколько мне известно.
5. I've no/not the slightest idea.	Понятия не имею.
6. There's no question about…	Несомненно, что…
7. If I am not mistaken …	Если я не ошибаюсь …
8. I know for sure that…	Я абсолютно уверен, что…
agreement	
1. I absolutely (completely, fully) agree with you.	Я абсолютно (полностью) согласен с Вами.
2. I am of the same opinion.	Я придерживаюсь того же мнения.
3. That's right (true)	Правильно …
4. I share your opinion.	Я разделяю ваше мнение.
5. That's exactly what I think!	Это именно то, что я думаю!
6. Yes, I feel the same about…	Да, у меня такое же мнение.
7.You're absolutely right.	Вы абсолютно правы.

disagreement	
1. I’m afraid you are mistaken. 2. Just the reverse 3. I fully (completely) disagree with you 4. I’m sorry, I can’t agree with you about…	Боюсь, Вы ошибаетесь Наоборот … Я совершенно с Вами не согласен. Простите, не могу с Вами согласиться по поводу…

Exercise 2. Make up a project «Technologies Used to Prevent Money Laundering»**.**

Unit 4. Risk management

Grammar: -ing; -ed forms Text 1. Risk management Text 2. Risk Assessment

Wordlist

Noun	Verb	Adjective	
accountability acquisition alignment assurance auditing benefit commitment complexity consequences consideration enterprise evidence flexibility framework governance hazard impact indebtedness legislation mainstay management mitigation objective performance probability reliability risk severity uncertainty	adjust adopt arise assess commence diminish enhance equip expose explicit increase manage maintain perceive predict set in survive tap into thrive trace verify	applicable coherent environmental measurable robust relevant valuable tangible	be a risky endeavour; cause-and-effect diagram; effect of uncertainty on objectives; finance-related risks; medium-sized enterprises; ignore risk treatment; market share; Probabilistic risk assessment; qualitative and quantitative analysis

Exercise 1. Recognize familiar words and phrases.

Risk avoidance, risk transfer, risk mitigation, risk acceptance, risk response, risk management process, to be identified and allocated in a well-defined manner, Risk identification, a cause-and-effect diagram, alignment, Sources of risk and potential consequences, project risk management, risk management effectiveness.

Exercise 2. Explain the difference between the following words.

1) hazard, risk;
2) access, assess;
3) structure, infrastructure;
4) affect, effect;
5) accept, except;
6) enable, able;
7) available, accessible;
8) sources, resources;
9) quality, quantity;
10) since, science.

Exercise 3. Match the terms and their definition.

1) risk identification, 2) checklists, 3) a cause-and-effect diagram, 4) an influence diagram, 5) hazard and operability study (HAZOP), 6) failure mode and effect analysis (FMEA).

---

1) a graphical representation of root causes of quality problems, where major causes of the final problem are grouped and broken down into detailed sources.

2) graphical representation of the structure of the decision context such that decisions, uncertain events, consequences and their interrelationships.

3) studying a situation to realize what could go wrong in the product design and development project at any given point of time during the project.

4) a trivial method of risk identification where pre-determined crucial points are examined for symptoms of potential risk situation.

5) provides a structure for determining causes, effects and relationships in a technical system.

6) an extension of FMEA where check words are applied to process parameters in order to identify safety and operational problems, usually in new systems.

Exercise 4. Translate the following words into Russian.

1) direct – direction – directional – directional – directly;

2) distribute – distribution – distributive – distributive – distributable;

3) serve – service – serviceable – serviceableness – unserviceable;

4) determine – determining – determined – determinant – determinable – determinate;

5) rectify – rectifying – rectified;

6) define – defined – defining – definite – definiteness – indefiniteness – definitive.

Exercise 5. Substitute the word in italics by its synonym (or synonymous phrase).

1. Managing risks in construction projects has some ***advantages*.**

a) drawbacks;

b) disadvantages;

c) strong points;

d) weak points.

2. The costs of these accidents are ***immense*** to the individual, to the employer and to society.

a) vast;

b) small;

c) long;

d) tiny.

3. It is critical that the description of governance ***reflects*** current arrangements.

a) depicts;

b) deflects;

c) gives;

d) represents.

4. Risk management is defined as «coordinated activities to ***direct*** and control an organization with regard to risk».

a) guide;

b) support;

c) enhance;
d) maintain.

5. **Objectives** can take the form of revenue targets, position with respect to competitors, financial reserves.

a) plans;
b) purposes;
c) rules;
d) achievements.

Exercise 6. Make up English-Russian pairs of the word groups equivalent in meaning.

I. 1) at any rate; 2) at great expense; 3) at least; 4) at once; 5) as soon as; 6) at the edge of; 7) by no means; 8) from now; 9) not (no) at all; 10) in general; 11) in the long run; 12) let alone; 13) in full; 14) of necessity; 15) of one's own; 16) on the one hand … on the other hand; 17) some day; 18) that long.

II. 1) в конечном счете (в далеком будущем); 2) в любом случае; 3) вообще; 4) как только; 5) когда-нибудь; 6) на грани; 7) никоим образом; 8) оставляя в стороне; 9) полностью; 10) отныне, с данного момента; 11) по меньшей мере; 12) по необходимости; 13) с большими затратами; 14) собственный; 15) совсем не; 16) с одной стороны … с другой стороны; 17) сразу; 18) так долго.

Exercise 7. Identify the predicate and Participle II and translate the following sentences.

1. The method applied increased the accuracy of the results. 2. Risks associated with a complex system, such as a nuclear power plant, may involve long chains of events. 3. After a heated discussion the company applied the method improved by their economist. 3. The scientist theoretically predicted complicated interaction between the components involved in the process. 4. For nested systems, the reliability of each subsystem must be assessed independently, and then all of these values aggregated to determine overall system reliability. 5. Consequently, methods such as fault and event trees have been developed to facilitate such analysis. 5. Once the system is understood, it is time to build a list of internal initiating events – abnormal events within the system, that could result in hazard exposure if not properly remedied. 6. The crystal produced revealed cracked faces. 7. We identified two more possible

consequences: the transactions either succeeded or failed. 8. Suppose that the data obtained in Step 9 included the following probability and severity information, to be added to the event tree. 10. Probabilistic risk assessment or similar analysis, if properly conducted on a suitable subject, does provide a valid, consistent measure of risk, but risk perception and risk acceptability are also important.

Exercise 8. Identify the -ing structures and give Russian equivalents of the relevant part of the sentence.

1. For all these reasons, deciding exactly what to include, and how to treat it, can be difficult. 2. An event tree is a diagram depicting all the possible consequences of an initiating event. 3. Such a tree is created by starting with the initiating event and identifying all of its relevant consequences, then systematically treating each consequence as a new event and identifying its consequences, and so on. 4. In the real world, however, managing risks frequently requires more than a series of calculations indicating something is sufficiently «safe». 5. In Economics literature,

those who desire risks are called «risk-seeking», while those who avoid risks are called «risk-averse». 6. In addition to (or even instead of) the average expected gain, they are considering the prospects of the full gain and loss, how they would feel in either case. 7. The availability and overconfidence biases should not be viewed pejoratively; they are simply properties of human thinking. 8. To conclude, here are a few tips to keep in mind when communicating about risk. 9. Risk identification is studying a situation to realize what could go wrong in the product design and development project at any given point of time during the project. 10. Developing nations in particular, experience pervasive risk of devastation, human and property loss resulting from human and natural disasters.

Exercise 9. Translate the sentences, using passive structures and the verbs: to affect, to allow, to attend, to develop, to deal with, to face, to follow, to make use of, to refer to.

1. За докладом последовала бурная дискуссия. 2. На скорость передачи информации влияет множество других факторов. 3. Этот вопрос будет подробно рассмотрен в главе III. 4. На этой стадии мы столкнулись с новыми трудностями. 5. Ему не дали возможности

закончить эту транзакцию. 6. В последнее время этот метод в управлении рисками часто упоминается во многих статьях. 7. Для того чтобы преодолеть эти недостатки, использовали новую методику, специально разработанную для данного эксперимента.

Exercise 10. Translate the sentences from Russian into English.

1. Проблема была впервые поставлена в XXI веке. 2. Предполагается, что полученные расчетные данные были проверены экспериментально. 3. Теория была принята большинством ученых после того, как были получены новые доказательства в ее поддержку. 4. В статье представлены новые данные относительно механизма этого процесса. 5. Это расхождение можно объяснить разными методиками измерения. 6. В работе использован новый метод расчета этого параметра и предложена новая модель процесса. 7. Особое внимание уделено сравнению экспериментально полученных результатов с результатами, предсказанными теоретически.

Exercise 11. Identify the structures paying attention to the -ing forms and translate the sentences.

1. Every new idea is immediately taken up and developed further, forming the initial point of an avalanche-like process. 2. What is worth doing is worth doing well. 4. At this stage innovation becomes a group and not an individual activity, involving both a sophisticated body of information and a sophisticated technology. 5. Soon Piet de Curie joined Marie Curie in her search for the “mysterious” substance, giving up his own research. 6. It is no good stressing a paradox if you wish to excite curiosity of the audience unprepared for the lecture. 7. Some people have been so scared reading about harmful effects of smoking that they gave up reading. 8. The editor could not help detecting many errors both of fact and of thinking. 9. Are these prognoses really worth making? 10. To find out more about the space scientists sent little moons, or satellites, circling in orbits above the Earth.

Exercise 12. Identify the Gerund and Participle I and translate the sentences.

1. Noticing relationships in his observations, the scientist attempts to classify and explain them. 2. Noticing relationship in his observations is

very important for every scientist. 3. Establishing relationship between the phenomena of the Universe is a major task of theory. 4. Realizing the necessity for a different approach the scientists reluctantly abandoned the project. 5. Confining his attention to one problem the economist will surely achieve its solution much sooner. 6. Putting the discovery to use sometimes requires more effort than making it. 7. Pointing out their mistakes to some people is often quite difficult. 8. Nobody can avoid making occasional mistakes. 8. Unfortunately the advantage of joining efforts for a complicated job is not always understood. 9. By realizing the threat to our information we have made the first step to its security. 10. The success of any risk assessment depends largely on precisely defining its objective.

Exercise 13. Identify Gerund and Participle I and translate the sentences.

1. Some problems can be solved only by the world economists joining their efforts. 2. Such problems can be solved only by an economist fully realizing the possible danger. 3. A brain-storming session consists in everybody's proposing as many, and as wild, ideas as possible, without being concerned as to whether they are workable. 4. The results of the risk assessment depended upon his having applied the proper technique. 5. The idea of economists' being responsible for most ills of the present day situation is unfortunately quite popular. 6. Let's proceed by dividing research into three stages and examining each stage to find what functions of the risk assessment process may be automated without endangering creativity. 7. Such a configuration, in addition to being amenable to analytical treatment, has significant practical importance.8. Finding an adequate solution to this most urgent economical problem will surely require much time and still more effort.

Exercise 14. Read and analyze the sentences.

1. Such a configuration, in addition to being amenable to analytical treatment, has significant practical importance. 2. His report resulted in establishing a new mechanism of the process. 3. Some people say that theory is a device for saving time. 4. The 21st century has witnessed the economist becoming the most valued member of society. 5. It is believed that there is hardly any chance of there being a mistake in these

calculations. 6. Mathematization of science is witnessed in almost all its branches, with specialists in humanities hurriedly joining the process. 7. The project abandoned, the leadership in this field passed to another institute.8. Methods employed in solving a problem are strongly influenced by the risk assessment objective. 9. The inquiry could be greatly helped by distinguishing two different classes of risk assessment techniques.

Exercise 15. Choose the proper form of the Participle.

1. Risk management is one of the nine knowledge areas (propagated, propagating) by the Project Management Institute. 2. Construction projects are inherently complex and dynamic, and (involving, involved) multiple feedback processes. 3. This naturally creates problems and confusion for even the most (experienced, experiencing) project managers and contractors. 4. Risk identification is the first and perhaps the most important step in the risk management process (identifying, identified) the source and type of risks. 5. (Combined, Combining) the fuzzy logic and a work breakdown structure, the authors grouped risks into six subsets: local, global, economic, physical, political and technological change. 6. The risks are (categorizing, categorized) into such groups: technical, external, organizational, environmental, or project management. 6. Generally two broad categories, namely, qualitative and quantitative analysis are (distinguished, distinguishing) in literature on risk assessment. 7. Event tree analysis is a graphical representation of potential consequences (arising, arisen) from a failure where possible consequences are generated and broken down from an initial event.

Reading

TEXT 1

Exercise 1. Answer the questions before reading the text

1. What is risk management?
2. Why is it the most difficult aspect of project management?
3. What are the key elements of risk management?

Risk management

Risk management is probably the most difficult aspect of project management. A project manager must be able to recognise and identify the root causes of risks and to trace these causes through the project to their consequences. Furthermore, risk management in the construction project management context is a comprehensive and systematic way of identifying, analyzing and responding to risks to achieve the project objectives.

The use of risk management from the early stages of a project, where major decisions such as choice of alignment and selection of construction methods can be influenced, is essential.

The benefits of the risk management process include identifying and analyzing risks, and improvement of construction project management processes and effective use of resources.

The construction industry is heterogeneous and enormously complex. The success parameters for any project are in time completion, within specific budget and requisite performance (technical requirement). The main barriers for their achievement are the change in the project environment. The problem multiplies with the size of the project as uncertainties in project outcome increase with size.

Large construction projects are exposed to uncertain environment because of such factors as planning, design and construction complexity, presence of various interest groups (owner, consultants, contractors, suppliers, etc.), resources (manpower, materials, equipment, and funds) availability, environmental factors, the economic and political environment and statutory regulations.

Construction projects can be unpredictable. Managing risks in construction projects has been recognized as a very important process in order to achieve project objectives in terms of time, cost, quality, safety and environmental sustainability.

Project risk management is an iterative process: the process is beneficial when is implemented in a systematic manner throughout the lifecycle of a construction project, from the planning stage to completion.

A typical risk management process includes the following key steps: Risk identification, Risk assessment, Risk mitigation, Risk monitoring.

Risk identification is the first and perhaps the most important step in the risk management process, as it attempts to identify the source and type of risks. It includes the recognition of potential risk event conditions in the construction project and the clarification of risk responsibilities. Risk identification develops the basis for the next steps: analysis and control of risk management. Corrects risk identification ensures risk management effectiveness.

Techniques for risk identification

Risk identification is studying a situation to realize what could go wrong in the product design and development project at any given point of time during the project. Sources of risk and potential consequences need to be identified, before they can be acted upon to mitigate.

Checklists are a trivial method of risk identification where pre-determined crucial points are examined for symptoms of potential risk situation. These are simple to use and usually evolve over time through contributions from various functional experts and collective experiences.

An influence diagram is graphical representation of the structure of the decision context such that decisions, uncertain events, consequences and their interrelationships are graphically enumerated.

A cause-and-effect diagram is a graphical representation of root causes of quality problems, where major causes of the final problem are grouped and broken down into detailed sources. Cause-and-effect diagrams are easy to use, they do not provide a foundation for further analysis such as relative importance of individual causes of a problem.

Failure mode and effect analysis (FMEA) provides a structure for determining causes, effects and relationships in a technical system. FMEA is used to determine failures and malfunctions through exploration of failure modes, consequences of a system component failure so that solutions for rectifying these problems can be visualized.

Hazard and operability study (HAZOP) is an extension of FMEA where check words are applied to process parameters in order to identify safety and operational problems, usually in new systems. Check words create other perspectives to the overall process and focus attention on unforeseen areas in the process.

In risk management for projects, HAZOP can be applied by considering project parameters such as strategy, budget and schedule to identify risk situations.

Event tree analysis is a graphical representation of potential consequences arising from a failure where possible consequences are generated and broken down from an initial event.

In project risk analysis its application is similar to fault tree analysis and works only on small zone of influence of potentially damaging consequence arising from a risk event.

Exercise 2. Look through the text to answer the questions.

1. What is risk management?
2. What are the benefits of the risk management process?
3. When is the use of risk management essential?
4. What are the success parameters for any project?
5. What are the main barriers for the achievement of the success parameters?
6. Why are large construction projects exposed to uncertain environment?
7. When is the process of project risk management beneficial?
8. What are the major elements of a risk management process?
9. What is the most important step in the risk management process?
10. What are the techniques for risk identification?

Exercise 3. Read the text and complete the sentences.

1. A project manager's responsibilities include…
2. Risk management in the construction project management context is a way of ….
3. The problems with success achievement increase with ….
4. Risk identification includes….
5. Risk identification examines….
6. Checklists are a usual way of risk identification when ….
7. An influence diagram is ….
8. A cause-and-effect diagram means….
9. The purpose of FMEA is to ….
10. HAZOP can be used by ….
11. In project risk analysis its application is …

Exercise 4. Give the English equivalents for the following.

Управление риском, управление проектом, выявлять риск, неоднородный, техническое задание, условия реализации проекта, неопределенность, результат проекта, рабочая сила, нормативные акты/положения, экологическая устойчивость, внедрять, уменьшение риска, график линии влияния, причинно-следственная диаграмма, анализ видов и последствий отказов, исследование опасности и работоспособности, дерево событий.

Exercise 5. Find and translate the paragraphs in which:

1. The term «risk management» in the construction project management is defined.
2. The importance of risk identification is explained.
3. The term «check list» is explained.
4. The term «cause-and-effect diagram» is defined.
5. The FMEA abbreviation is given.
6. The HAZOP abbreviation is given.
7. The term «event tree analysis» is defined.

Exercise 6. Read the text. Make the following steps to write the précis of the text.

1. Read the sentence that expresses the main idea of the text.
2. Examine each paragraph and point out the topic sentences.
3. Read the topic sentence or sentences in each paragraph.
4. Read the key words in each paragraph.

Exercise 7. Read the text and make up the summary using the following phrases.

1. … offers a detailed and practical introduction to …
2. Risk management is the focal point because …
3. … is an essential guide to …
4. … provides the reader with (details).
5. The text could be divided into … parts, in which …
6. The text explains the importance of risk management by…
7. It defines the first key element of risk management as …
8. It introduces techniques of risk identification as the following …
9. … has a major impact on…
10. This supports the idea that …

TEXT 2

Risk Assessment

Concept/Types of Risk

1. The notion of risk is basically a combination of two concepts: probability and severity.

That is, we decide how risky something is by asking two questions:

– How likely is this to happen? (probability)

– How bad would it be if this did happen? (severity)

2. Before going further, let us clarify a few terms. A *hazard* is anything potentially costly, harmful, or undesirable. Hazards lead to risks. The connection between hazard and risk is an *event* – a situation in which someone/thing is exposed to the hazard. It is important not to confuse these terms. A pot of boiling water is a hazard, since it could cause harm. How risky is it? We cannot say, without information about who/what is exposed to it. If we specify an event, such as a person bumping the pot (and getting burned), then we can assess the probability and severity, and from these the risk (note that both are required; either alone is insufficient, i.e., uncertainty does not necessarily mean risk).

3. Risk can be assessed either quantitatively or qualitatively. If both the probability and severity can be quantified, the risk is simply the product: risk = probability * severity. For example, if the probability of a computer server «crashing» in a 24-hour period is 10-6, and if the cost of a crash is estimated to be $2,000,000 (for lost revenue while the system is down, plus repairs), then the risk of relying upon such a server is about $2 per day. This could be compared with the cost risk of an alternative.

4. Assessing risks is not always straightforward, however. The probability or severity of an event may not be known (e.g., the probability that your car will break down tomorrow), or not agreed-upon (e.g., the severity of global warming). Many risks may be associated with a given hazard. Risks associated with a complex system, such as a nuclear power plant, may involve long chains of events. For all these reasons, deciding exactly what to include, and how to treat it, can be difficult.

5. Finally, there are many different types of risk – as many as there are values that can be threatened. Among the most prominent types are safety, cost, schedule, technical, and political risk, and most decisions involve more than one of these. An important part of risk management is deciding which types of risk to assess, and how they should be compared to make decisions.

Probabilistic Risk Assessment

6. Probabilistic risk assessment (PRA) is a quantitative procedure used to evaluate technical risks. The basic process involves five steps:

1. Identify hazards and initiating events
2. Identify mitigating safety measures Trace possible chains of events
3. Quantify all individual probabilities and severities
4. Aggregate probabilities and severities, and calculate risks

7. A principal component of PRA is reliability analysis. *Reliability* is simply a different form (the reciprocal) of probability of failure. Thus it is related to risk. (Note: it is a common misconception that reliability is simply risk in a different form. This is not the case, because reliability does not contain severity information.) As systems grow in complexity, accounting for the effects of various combinations of subsystem failures quickly becomes very complicated. Consequently, methods such as fault and event trees have been developed to facilitate such analysis.

8. A formal procedure for conducting PRA is specified in ten steps, it addresses more details than the basic description above, but it is fundamentally equivalent.

1. Methodology Definition
2. Familiarization and Information Assembly
3. Identification of Initiating Events
4. Sequence or Scenario Development
5. System Analysis
6. Internal Events External to the Facility
7. External Events
8. Dependent Failure Considerations
9. Failure Data Analysis
10. Quantification

Exercise 8. Read the text to answer the questions.

1. What two ideas does the notion of risk assessment include?
2. What is the difference between a hazard and a risk?
3. How can you assess risk qualitatively?
4. Why is assessing risk not always clear/easy?
5. What are the most obvious types of risk?
6. What are the key elements of PRA?
7. What is the difference between a reliability and a risk?
8. What methods help reliability analysis?
9.What does A formal procedure for conducting PRA include?

Exercise 9. Read the text without consulting the dictionary. Pencil-mark the unknown words, if any, and try to deduce their meaning relying on the context. Consult the dictionary to see if you were right.

Exercise 10. Examine paragraph 1, 2 do the following.

1. Give the English equivalents to: вероятность, серьезность, опасность, необходимо, недостаточный, неопределенность.

2. Identify the part of speech of the following words. State their functions in the contexts:

a… basically…
b… someone/thing…
c… without information…
d… getting burned…
e…either…

3. Express the main idea of the paragraph.

Exercise 11. Examine paragraph 3 and give three of your own examples to use the formula of quantitative risk assessment.

Exercise 12. Examine paragraph 4 to identify the following structures. State their functions in the sentences:

a) assessing risks
b) not agreed-upon …
c) associated with…
d) deciding…
e) what to include…

Exercise 13. Read paragraph 5, 6 and give definitions of the following words.

Value, safety, cost, probabilistic, initiating, mitigating, aggregate.

Exercise 14. Examine paragraphs 7 and give Russian equivalents.

Reliability analysis; reciprocal; probability of failure; common misconception; accounting for; fault tree; event tree; facilitate.

Exercise 15. Read paragraph 8 and translate it into Russian.

Exercise 16. Write the précis of the text.

Exercise 17. Make up the summary of the text using the following phrases:

1. The text is entitled…
2. The text deals with the problem of …
3. The main focus is on …
4. The author reveals...
5. The text contains the description of ...
6. Summing it up…

Written Practice

Exercise 1. Learn to write CV

CURRICULUM VITAE

NAME: Vladimir Popov
DATE OF BIRTH: 11 October 1980
ADDRESS: Pushkinskaya street, 55/15
TELEPHONE NUMBER: 255-55-55
MARITAL STATUS: single
HEALTH: excellent
EDUCATION: 1999-2008 – secondary school № 32 (specialization in physics). 2008- 2013 University “MEPHI”.
WORKING EXPERIENCE: 2013-2019 assistant
OTHER QUALIFICATIONS: communicative English
HOBBIES: computer

REFERANCES: the following people have given (provided) references for me:
Maria I. Ivanova, teacher of English, school №35, tel. no. 333-12-23
Sergey P. Petrov, principal, tel. 211-450-66

Exercise 2. Learn to fill in the following form.

Surname **…..**
First name (s)….
D.O.B. (Date of birth) ….
Marital status …(s ingle, married, divorced)
Children…
Address …
Tel No …
Education and Further studies …
Dates / Schools/ colleges/universities / Qualifications (name and address) / Experience
Dates Place of work job pay (with address)
Signature

Exercise 3. Practise the following conversation. Try to create the similar one.

Exercise 4. Learn to write Preliminary Registration Form.

Name (Names in full) _____Title_____
Official address:_____
Company: _____
Street_____ City_____ Post. Code _____ Country_____
I intend to participate in the 5th International Congress of Telecommunications:
__ with an oral communication
__ with a poster of products
__ with an exhibition display
__ with an announcement in the Abstract book of the Congress
__ as listener
I need in hotel accommodation:
__ single
__ twin
__ suite
Arrival: Date _____ Time_____
Departure: Date _____Time_____
Signature _____Date _____

Payment is made on: By Bank transfer to: ICT 09 – Banque Rhone-Alpes – Lyon Center; Bank code: 10 468 – Branch code: 02 353; Account Number: 19555- Key code: 31

Exercise 5. Fill in the Registration form.

Registration Form

To be returned **before July 15th, 2019** to**:**
Package Organization
53 rue Vauban. F – 69006 Lyon
Tel: 333 (0) 4 78 24 18 06 – Fax: 33 (0) 4 74 72 18 33
AFTER JULY 15TH, 2019, PLEASE REGISTER ON SITE
Participant:
Name:_____
Position Held_____
Organization:_____
Address: _____
Zip code:_____ City: _____ Country:_____
Tel:_____ Fax:_____
Accompanying Person (s):
First Name:_____ Name:_____
First Name: _____ Name:_____
Registration (Please circle the correct amount)

	Until March 31, 2009	After March 31, 2019
ICT member	2000 $	2500 $ _____
ICT non member	2600 $	3500$_____
Student	600 $ until July 15th, 2019	
New investigator this rate is not be available on site._____		
Accompanying person	750 $	750$

Settlement:
Registration_____= $
Bank Charges (for cheque and bank transfer from abroad)__170$_____= $
Total to pay_____=$
By Bank transfer to: ICT 09 – Banque Rhone-Alpes – Lyon Center;
Bank code: 10 468 – Branch code: 02 353;
Account Number: 19555- Key code: 31
No registration will be processed without corresponding settlement.
Date Signature

Exercise 6. Write an essay «A guideline to PRA: which steps are the most important».

The materials for your essay

TEXT 1-10

This section presents a formal procedure for conducting PRA. Specified in ten steps, it addresses more details than the basic description above, but it is fundamentally equivalent. We will discuss each step in turn.

1. Methodology Definition

The first step in preparing a PRA is to review the analytical options: using computer programs, consulting experts, etc. The requirements for the PRA and the advantages and disadvantages of each analytical option should then be considered, and the most cost-effective option selected.

2. Familiarization and Information Assembly

Next, it is important to become familiar with the system or process under consideration.

The physical layout, standard procedures, safety measures, etc. should all be investigated. It is essential to understand how things are supposed to work, what could go wrong, and what might happen if it did. It is also valuable to review the details of any failures that have occurred in the past. All of this information should be organized and documented to facilitate future review and provide a solid foundation for the PRA.

3. Identification of Initiating Events

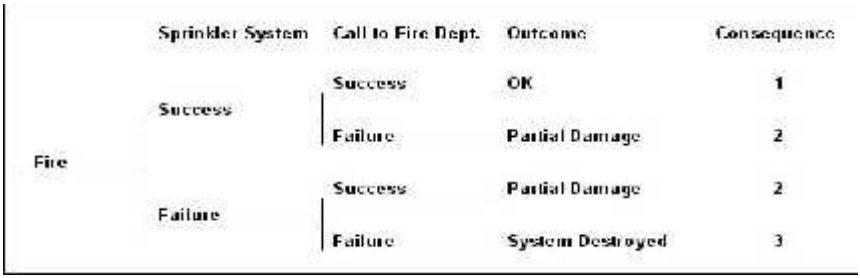
Once the system is understood, it is time to build a list of internal initiating events – abnormal events within the system that could result in hazard exposure if not properly remedied. There are a number of ways to approach this, from «what-if» brainstorming to Failure Mode and Effects Analysis (FMEA).

The important thing is to identify as many plausible internal hazards and associated events as possible. For engineering systems, a common approach is to identify hazards with barriers, and the threats they pose to those barriers, but this is not always necessary.

If the list of initiating events becomes extensive, it would probably be wise to group similar events together. For example, categories can be

defined for all events that break the same barrier, contribute to the same risk, or require the same corrective actions. This will simplify the rest of the analysis, focusing concentration on significant categories instead of redundant events.

4. Sequence or Scenario Development



The next step is to investigate the consequences of internal the initiating events. This is usually achieved through event tree analysis. An event tree is a diagram depicting all the possible consequences of an initiating event. Such a tree is created by starting with the initiating event and identifying all of its relevant consequences, then systematically treating each consequence as a new event and identifying its consequences, and so on. This structure of possible consequence events branching out to more possible events at each level forms a «tree.» Although they can quickly grow large, trees are valuable because they enable us to trace causal paths of events.

A simple example event tree presented as the initiating event is a fire, for which we identify two possible consequences: activate the sprinkler system and call the fire department. We begin with the sprinklers as the next event level.

Here we identify two more possible consequences: the sprinklers either succeed or fail. For either result we then go to the next branch, the fire fighters, for which we also identify succeed or fail consequences. (This branch is attached to both branches from the sprinkler event, because whether the sprinklers succeed or not, the fire company is called.) At this point the tree stops, because there are no more consequences to include.

To complete the tree, we now label all of the final outcomes. If the sprinklers succeed, then if the fire fighters succeed the system will be

OK, or if the fire fighters fail there will be only partial damage. However if the sprinklers fail to begin with, then if the fire fighters succeed there still will be partial damage, or if the fire fighters also fail the system will be destroyed. Thus we can see that an initiating event of a fire could lead to any of three ultimate consequences – the system could be OK, partially damaged, or destroyed – and we can see the paths, or event sequences, that lead to each.

This is only part of the functionality of event trees. In later steps of the PRA, we will return to each event tree and define the branch probabilities (in this example, these would be the sprinklers' and fire fighters' probabilities of success), and then aggregate them to calculate the likelihood of each outcome. Finally, we will quantify the severity of each outcome, and determine the overall risks. But at this point, the goal is just to trace the paths of possible consequences from initiating events. To complete Step 4, such an event tree must be created for each initiating event identified in Step 3.

5. System Analysis

In many cases, event trees contain important branch points, such as where a critical safeguard may or may not function, for which we do not have much information. In the example above, we might be concerned with exactly how likely the sprinkler system is to succeed. To gain such information, we must conduct internal system analysis. A useful approach in many situations is fault tree analysis. A *fault tree* is similar to an event tree in that it starts with an event, but instead following the consequences, it traces the causes.

An example fault tree for the sprinkler system begins with the problem we wish to analyze, known as the «top» fault or event, which in this case is the sprinklers failing to extinguish the fire. What could cause this? The sprinklers never get activated, or they are activated but fail to operate. These «triggering» events are linked to the top fault with an "OR-gate" because it only takes one or the other to cause the fault.

Now we add a branch tracing their causes. The sprinklers never get activated if the automatic sensors fail and no manual activation occurs. These are linked through an «AND-gate» because it takes both of them to cause the fault. Finally, the sprinklers fail to operate, even if activated, if water does not reach them OR if their valves fail to open.

Obviously we could continue the tree further, listing causes for each of these third-level triggering events, but at some point we have to stop.

(This point is a judgment call; it depends on what is of interest and what information is available.) We call the triggering events at the bottom (or at the ends of the branches, since the tree could be oriented in any direction) «basic events» or «root causes».

We assign probabilities to each root cause, and then combine these probabilities, to get probability of the event one level up. We proceed in this way, level by level, until we finally have the probability of the top fault. Now we can update our event trees with this improved information.

6. Internal Events External to the Facility

This step simply takes into consideration any events that originate within the system but then spread beyond the facility boundaries. Some examples might be internal fires, floods, or energy discharges. In most cases, there will be few events of this type, but any that are included should be analysed just like the internal events in Steps 3-5.

7. External Events

Here, we simply consider the last category of events, those originating outside the system, such as storms, seismic events, transportation events, etc. As before, any new events that are included should be analyzed just like the internal events in Steps 3-5.

8. Dependent Failure Considerations

A common risk management practice is the installation of redundant systems. This increases reliability by creating multiple success paths – but only as long as the systems are truly independent. If there is any dependency, a failure in one unit could compromise another.

There is sometimes a risk of such failure coupling even in systems thought to be independent, if they share the same operating environment or have functional or spatial links. Accordingly, it is important to carefully look for elements that could be prone to common-cause failures, and to make sure that they (and their potential dependencies) are explicitly incorporated in fault and event trees wherever applicable.

9. Failure Data Analysis

The next step is to obtain failure data for all of the events listed in all fault and event trees. There are a variety of sources of failure data. Past experiences are usually best (if any failures in this, or other similar systems, have occurred), but some values must be estimated from generic failure data, or based on expert opinion. Data should also be obtained and included for outages due to test, repair, and maintenance.

10. Quantification

To complete the PRA, the information from Step 9 is applied to fully quantify all fault and event tree sequences. These are then reduced and combined to obtain probability and severity information for the desired system elements, operations, and events. For example, let us return to the event tree developed in Step 4. Suppose that data obtained in Step 9 included the following probability and severity information, t be added to the event tree.

P (sprinkler system success): 0,8

P (fire dept. success | sprinkler success): 0,95

P (fire dept. success | sprinkler failure): 0,5

Cost (fire handled OK): –$1,000

Cost (partial damage): –$500,000

Cost (system destroyed): –$3,500,000

Now it is simply a matter of calculation: the overall probability of an OK outcome (only $1000 damage) is (0.9)(0.95) = 85.5 %; the overall probability of a Partial Damage outcome ($500k damage) is (0.9)(0.05) + (0.1)(0.7) = 11.5 %; and the overall probability of system destruction ($3.5M damage) is (0.1)(0.3) = 3 %. Then, combining the probability and severity information, we can calculate that the overall average risk of fire damage: (.855)(–$1,000) + (.115)(–$500,000) + (.03)(–$3,500,000) = –$163,355.

Finally, if any risk levels are not acceptable, the fault and event trees can be used to identify problem areas and/or common sequences leading to undesirable outcomes. These can then be targeted for risk management efforts. For example, if the risk calculated above was deemed too high, the sprinkler system could be targeted for improvement (to increase its probability of success). Note that additional system analysis (Step 5) may be required to determine exactly how to achieve the desired improvements.

Exercise 7. Make up a project: My own event and fault trees for the following industries.

1. Construction
2. IT
3. Food

Алевтина Георгиевна Строилова
Оксана Николаевна Овсянникова
Оксана Данияловна Агамова
Елена Георгиевна Иванова

Английский язык
Учебное пособие для студентов экономического направления

Корректор М.В. Макарова

Подписано в печать 20.08 2019. Формат 60x84 1/16
Уч.-изд. л. 7.5. Печ. л. 7.5. Изд. № 038-1.

Национальный исследовательский ядерный университет «МИФИ»
115409, Москва, Каширское ш., 31