УДК 37.016

Яроцкая Людмила Владимировна
ФГБОУ ВПО «Московский государственный лингвистический университет»
Институт права, экономики и управления информацией
Кафедра лингвистики и профессиональной коммуникации в области права
Россия, Москва
Кандидат педагогических наук, профессор
E-Mail: lvyar@yandex.ru

Желнов Илья Игоревич
ФГБОУ ВПО «Московский государственный лингвистический университет»
Россия, Москва
Заведующий кафедрой информационных технологий
Кандидат военных наук
E-Mail: jelnov-i@yandex.ru

К вопросу о моделировании социокультурного контекста в предметном поле «защита информации» (на примере учебного пособия по иностранному языку)

Аннотация: В статье авторы обобщают свой опыт моделирования социокультурного контекста в предметном поле «Защита информации» при реализации межкультурной парадигмы лингводидактики.

Авторы обосновывают необходимость комплексного подхода к разработке учебников и учебных пособий, направленных на формирование межкультурной иноязычной профессиональной коммуникативной компетенции, и в качестве основного критерия отбора текстов называют их информативную полиперспективность – взаимосвязанное рассмотрение основных процессов и закономерностей, лежащих в основе развития специального знания в области технологий защиты информации с древнейших времен до наших дней, в общеисторическом, специфическом этнокультурном и предметно-центрическом контекстах.

Ключевые слова: Защита информации, социокультурный контекст, межкультурная иноязычная профессиональная коммуникативная компетенция, критерии отбора текстов, информативная полиперспективность.

Вопрос о содержательном аспекте специализированных текстов, предлагаемых в учебных пособиях по иностранному языку, являлся предметом нашего рассмотрения в ряде научно-педагогических публикаций [3, 4, 5], однако важнейший аспект – моделирование социокультурного контекста развития научного знания – требует, на наш взгляд, особого внимания авторов учебников и учебных пособий, поскольку открывает значительные возможности для формирования профессиональной личности. В этой связи ценным представляется мнение А. А. Вербицкого, основоположника контекстного подхода в обучении, о необходимости отражения в содержании обучения «противоречивого движения содержания научного знания (предметный контекст), развертываемого как борьба мнений, позиций, научных школ или отдельных ученых в истории науки, как их диалог (социальный контекст). С помощью моделирования этих контекстов студент приобщается к объективным противоречиям науки, развивается теоретически и воспитывается как специалист» [1, с. 60]. Добавим, что наш опыт преподавания иностранного языка студентам различных специальностей показывает, что сопутствующая реализация также исторического, социокультурного и эмоционального контекстов неизменно привлекает студентов и повышает мотивацию учения. Если тексты содержат спорные положения, аргументацию, выводы или сведения, которые остались за рамками учебников и лекций по специальности, то открывается широкое поле для приложения студентами своих мыслительных способностей, для анализа, сравнения, выводов, появляется и естественное основание для дискуссии. На наш взгляд, нет ничего страшного в том, что на каком-то этапе студент сделает не тот вывод, которого от него ожидает преподаватель. Думающий человек все равно придет к обоснованным выводам, и это будут его выводы и его убеждения, а не умозаключения преподавателя, заученные студентом для удобства ответа на экзамене [4]. Более того, реализация межкультурной парадигмы лингводидактики предполагает приоритетную актуализацию именно этих контектсов [2, 5, 6, 7].

В данной статье приводится пример взаимосвязанного моделирования предметного и социокультурного контекстов развития специального знания в рамках пособия по иностранному языку «Информационная безопасность и защита информации: Учебное пособие для документоведов» [2].

Основной целью пособия является развитие дискурсивных умений, связанных с чтением оригинальной научной литературы по специальности, созданием профессионально значимых видов письменных речевых произведений, а также ведением беседы на профессиональные темы.

Главным критерием отбора текстов, представленных в пособии, явилась их информативная полиперспективность, предполагающая взаимосвязанное рассмотрение основных процессов и закономерностей, лежащих в основе развития специального знания в области технологий защиты информации с древнейших времен до наших дней, в общеисторическом, специфическом этнокультурном и предметно-центрическом контекстах [2].

Последовательность моделирования профессионально релевантных контекстов с помощью пособия «Информационная безопасность и защита информации: Учебное пособие для документоведов» определяется логикой развития предметно специализированного знания.

Система упражнений в стандартном разделе пособия включает предтекстовые упражнения, подготавливающие студентов к восприятию текста (снятие лингвистических и экстралингвистических трудностей), текст и блок послетекстовых упражнений.

Значительное место в пособии отводится работе над потенциальным словарем, в том числе специальными терминами, характеризующимися, как показывает проведенное автором пособия исследование, большим количеством производных и сложных слов.

Важнейшим этапом подготовки к чтению текста является самостоятельная работа студентов, связанная с созданием внутреннего контекста (фоновых знаний) для эффективного восприятия текста. В частности, студентам предлагаются проблемные вопросы, связанные с выяснением конкретно-исторических условий развития общества на определенном этапе, специфических условий той или иной культуры, самостоятельным выделением факторов, которые могли повлиять на развитие специальных знаний и практик в области технологий защиты информации, с обоснованием своего выбора. Содержание предъявляемого на следующем этапе текста, с одной стороны, базируется на этих фоновых знаниях, а, с другой – способствует их уточнению, коррекции и расширению.

Работа с текстом включает несколько ступеней, что связано с последовательным проникновением в его содержательную структуру (определение темы, озаглавливание, ответы на вопросы по содержанию и проблематике текста, анализ структуры текста, составление развернутого плана текста).

В каждом разделе пособия предусмотрены упражнения, направленные на развитие умений продуктивной письменной речи (написание резюме одного / нескольких источников, с критической оценкой содержания / без нее; написание заключения к тексту / серии текстов).

Развитие навыков и умений продуктивной устной речи может осуществляться на выбор студента как за счет рассмотрения дополнительных вопросов, связанных с исследуемой в тексте проблемой (расширение контекста), так и за счет углубленного анализа поднятых в тексте вопросов.

Анализ результатов опытного обучения, проведенного при активном использовании пособия «Информационная безопасность и защита информации: Учебное пособие для документоведов», подтверждает гипотезу авторов о том, что в структуре современного профессионально ориентированного учебника иностранного языка как определяющего средства обучения вполне реальным является достижение строгого баланса учебных, коммуникативных, когнитивных и профессиональных целей и средств их достижения, обусловленного их взаимными трансформациями в направлении обогащения коммуникативной иноязычной деятельности профессиональным содержанием [5].

Взаимосвязанное и динамичное моделирование предметного и социокультурного контекстов развития специального знания в предметном поле «Защита информации» в рассматриваемом пособии обеспечивается следующей структурой и последовательностью упражнений.

UNIT I

THE FIRST 3,000 YEARS

Section 1

Exercise 1.

A. Look up the word ‘crypt’ in an English-English dictionary. Analyze its meaning(s). What derivatives and compounds does it form? Put down the word, its derivatives and compounds into your exercise-book. Make sure you pronounce the words

correctly.

B. How are the following words formed? Can you guess what they mean? Make sure you pronounce the words correctly.

(a) A code, to code, to decode, to encode, a codebook;

A message, to message, a messenger;

A place, to place, to replace, replacement;

A form, to form, transformation, cuneiform (writing);

A cipher, to decipher, to encipher, unenciphered, encipherer, decipherer, encipherment, cipher-like, ciphertext;

(b) To intercept – interception; to substitute – substitution; to communicate – communication; to transmit – transmission; secret – secrecy;

(c) Plaintext, ideogram, steganography, checkerboard;

C. Is the meaning of the noun 'word' the same in the examples below? Is it countable or uncountable? Refer to an English-English dictionary to make sure your analysis is correct.

The Latin word for *a table* is *mensa*.

He sent word by messenger.

Exercise 2. Answer the questions.

1) What is cryptography? 2) What do you know about its origins? What brought it into being? 3) What makes cryptography a cutting-edge field at present? 4) How do cryptography and cryptology relate? What is cryptanalysis? 5) Who is considered the first known cryptanalyst in the history of humankind? 6) Do you happen to know the source that includes the world's first conscious reference to – as distinct from use of – secret writing? 7) What are the makings of a good cryptologist? Prove your point of view. 8) Read a paragraph from an advert of a book: *When the National Security Agency's invincible code-breaking machine encounters a mysterious code it cannot break, the agency calls in its head cryptographer, Susan Fletcher, a brilliant, beautiful mathematician. What she uncovers sends shock waves through the corridors of power. The NSA is being held hostage – not by guns and bombs, but by a code so complex that if released would cripple U.S. intelligence.* Do you think that the situation described is highly probable? What makes you think so? 9) Have you read books (or have you seen films) about cryptology or cryptanalysis? Did you enjoy them? 10) Have you ever tried cryptography and cryptanalysis? If so, do you mind sharing your experiences with the class?

Exercise 3.

A. Read the text. Think of a good title.

On a day nearly 4,000 years ago, in a town called Menet Khufu <…> The disconnected letters make no sense unless the parchment is rewrapped around a baton of the same thickness as the first: then words leap from loop to loop, forming the message.

(Compiled from *Kahn, D. The Codebreakers. The Story of Secret Writing. – New York: Macmillan Publishing Company, 1967. – 1164 p.*)

B. Refer to Exercise 2. Did you manage to answer all the questions? If you failed to do so, try to find answers in the

above text.

C. Read the text again. Divide it into logical parts. Write an outline of the text.

D. The text has no conclusion. In the text, find a paragraph that could serve as a good conclusion.

E. Prepare to discuss in detail the facts given in the text. Look up any words that you may not know but you may need to discuss the text in class. Make sure you pronounce the words correctly.

Exercise 4. Answer the questions.

(I)

1) Who opened the recorded history of cryptology? When and how did he do it? What was the most likely intention of so doing? 2) Which essential element of cryptography did that writing have? 3) What tendencies did transformations show as Egyptian civilization developed? What did those transformations have in common with the oldest known text of this kind? What new essential for cryptography was developed? 4) What is meant by *Madison Avenue technique*? Was it a success in Ancient Egypt? Why so? / Why not? 5) The combination of what components produced cryptography? 6) Why were the cryptography and cryptanalysis of that time compared to a game? Are they the same nowadays? What does the science of cryptology deal with? 7) Why is the story of cryptology called *the story of mankind*? Do you agree with the statement?

(II)

1) Was cryptography popular in ancient China? 2) Why did China, so far ahead of other civilizations in so many things, not develop cryptography? 3) What is described as a *form of steganography*? 4) What codes were used in actual cryptography in China? 5) Why did Genghis Khan never make use of cryptography? 6) What cryptologic episode with a Western alphabet took place in the history of China?

(III)

1) What forms of secret communication were practiced in India? 2) Who made the first reference in history to cryptanalysis for political purposes? 3) When and where did it take place?

(IV)

1) Why does the author say that Mesopotamia attained *a surprisingly modern language of cryptography*? 2) What made it so modern? 3) What is cuneiform writing?

(V)

1) What is typical of the Holy Scriptures as far as cryptology is concerned? 2) How are the two components of cryptography – transformation and secrecy – combined? 3) What paradoxical cryptogram is the Bible famous for? 4) Who is considered the first known cryptanalyst?

(VI)

1) How did ancient Greece contribute to cryptology? What were the Greeks the first to do? 2) According to the text, *one of the most important messages in the history of Western civilization was transmitted secretly.* What message was it? 3) Who established the first system of military cryptography? 4) What device considered the earliest apparatus used in cryptography did the Spartans employ? 5) In the text, we come across the term *transposition cipher*. What is it?

Exercise 5. Write a summary of the above text.

Exercise 6. Refer to your outline of the text (Exercise 3(C)). For each point of the outline write out key words and word combinations that may come in handy in retelling the text. Prepare to comment on the facts and enlarge upon the topic.

Section 2

Exercise 1.

A. What parts of speech are the following words derived from? How are the meaning and the word class of each changed?

Conversion, reduction, division, substitution, transposition, encipherment, to signal, to number, steganographic, manipulable.

B. Which word from the line below does not go with the rest?

Consonant, vowel, character, personality, letter, number, symbol, digit.

Exercise 2. Answer the questions.

1) Is it easy to recognize a word if it is spelt with all the vowels omitted? Is it easy to do the same with all the consonants omitted? Which is normally easier – to recognize a word with omitted vowels or with omitted consonants? Which contractions are the more common? Why so? 2) Have you ever tried any form of quick writing? What method did you employ? 3) What is communications security? Has it gained or declined in importance compared with ancient times? Why so? What methods can be used to provide it? Are there any ultimate methods to provide communications security? 4) What is the difference between transposition and substitution ciphers? Give examples. What are the pluses and the minuses of each type? 5) There is an opinion that *Julius Caesar impressed his name permanently into cryptology as he did into many other fields*. Do you happen to know about his contribution?

Exercise 3.

A. Read the text. Think of a good title.

The world owes its first instructional text on communications security to the Greeks. <…> ‘When Augustus wrote in cipher,’ said Suetonius, ‘he simply substituted the next letter of the alphabet for the one reqired, except that he wrote *AA* for *x*’ (the last letter of the Roman alphabet).

(Compiled from *Kahn, D. The Codebreakers. The Story of Secret Writing. – New York: Macmillan Publishing Company, 1967. – 1164 p.*)

B. Divide the text into logical parts. Write an outline of the text.

C. Prepare to discuss in detail the facts given in the text. Look up any words that you may not know but you may need to discuss the text in class. Make sure you pronounce the words correctly.

Exercise4. Answer the questions.

1) What people does the world owe its first instructional text on communications security? Do you think it was pure coincidence that it was produced by that people? 2) Who was the author of the

text? What kind of book was it? 3) What systems of communications security did he describe? 4) What did cryptographers of the 20th century borrow from the ancient Greek steganographic systems? Give examples. 5) What system of signaling was devised by Polybius? 6) What characteristics of the Polybius square have modern cryptographers found exceedingly valuable? Why is the square commonly referred to as *checkerboard*? 7) Are the above ciphers transposition or substitution ciphers? 8) What was Julius Caesar's contribution to cryptology? What ancient sources describe his experiences in communications security? 9) How did Julius Caesar improve on his technique? 10) Was Augustus, first emperor of Rome, as successful as his famous uncle?

Exercise 5. Write a summary of the above text.

Exercise 6. Refer to your outline of the text (Exercise 3(B)). For each point of the outline write out key words and word combinations that may come in handy in retelling the text. Prepare to comment on the facts and enlarge upon the topic.

Section 3

Exercise 1.

A. How are the following words formed? Can you guess what they mean? Make sure you pronounce the words correctly.

(a) Equal, unequal, to equal;

A catalog, to catalog;

Compile, compiler, compilation;

(b) Commoner, immortality, historian, chronicler. occurrence;

Horizontal, runic, veritable;

Inevitably, spontaneously, apparently, perpendicularly, diagonally, profusely;

Monalphabetic, heterogeneous, genealogical, pictographic.

B. Is the meaning of the noun 'culture' the same in the examples below? Is it countable or uncountable? Refer to an English-English dictionary to make sure your analysis is correct.

The people's literary culture was unique.

It is vital for people from different cultures to learn to understand each other better.

C. Which (a) word / (b) phrase in each of the groups below does not go with the rest?

(a) To reverse, to shuffle, to garble, to thrive;

(b) Reciprocal substitution between consecutive letters of the alphabet, pictographic writing, hieroglyphic replacement, monalphabetic substitution, equation of the names of birds with the letters of the alphabet, equation of the letters of the alphabet with the names of the 28 astronomical lunar mansions.

Exercise 2. Answer the questions.

1) What kinds of scripts do you know? Are they Latin or non-Latin scripts? Which is the more widely-spread script – the Cyrillic or the Roman alphabet? 2) Specify the notions of *ciphertext* and *plaintext*. Can the change of the script alone refer a text to the opposite category? 3) What is a hardy plant? What can the word combination mean when used metaphorically? What fields of human activity do you think it can refer to? Prove your point of view. Do you think cryptography can be compared to a hardy plant? 4) What is necessary for a phenomenon to survive throughout history? 5) Do you know any cryptographic texts that are exhibited in museums?

Exercise 3.

A. Read the text. What is its topic?

It must be that as soon as a culture has reached a certain level, probably measured largely by its literacy, cryptography appears spontaneously <…> Methods for enciphering them are catalogued in the *Book of Ballymote*, a 15th-century compilation of historical, genealogical, and other facts of importance.

(Compiled from *Kahn, D. The Codebreakers. The Story of Secret Writing. – New York: Macmillan Publishing Company, 1967. – 1164 p.*)

B. Find the topic sentence in the above text. How is it developed?

Make a detailed list of the developers.

C. Prepare to discuss the facts given in the text. Look up any

words that you may not know but you may need to discuss

the text in class. Make sure you pronounce the words correctly.

Exercise4. Answer the questions.

1) What two explanations for the occurrence of cryptology does the author give? Which does he find the more probable? Do you share the author's opinion? 2) What do you think the author of the text mean by writing that 'cryptology appears spontaneously'? How does he prove it? Are his examples convincing to you? 3) What scripts are mentioned in the text? What peoples employed them? Make a list of the proper names used to describe the scripts and the peoples. 4) What ancient cryptographic treasure does the Metropolitan Museum of Art in New York possess? What is the thing noted for? What makes it a unique exhibit? 5) What non-Latin scripts of Europe made use of different ciphers in the past? Where do we come across them most often? 6) What fact(s) do you think the wide spread of cryptology testifies to? Prove your point of view.

Exercise 5. Write a summary of the above text.

Exercise 6. Prepare to comment on the facts given in the text and

enlarge upon the topic.

Section 4

Exercise 1.

A. How are the following words formed? Can you guess what they

mean? Make sure you pronounce the words correctly.

Assertion, concealment, backward, hieroglyphics, incurable, to engender, to attempt, to balance, loanword.

B. Account for the use of the italicized words in the following

examples.

Among *the Arabs*, the *Arab* world; *Arabic* loanwords, *Arabic* letters, *Arabic* numerals, the *Arabic* language; *Arabia*.

Exercise 2. Answer the questions.

1) What period do we refer to as *the Dark Ages*? How does it relate to *the Middle Ages*? 2) How did Western civilization develop in those times? 3) Do the names of *Roger Bacon* and *Geoffrey Chaucer* ring a bell? If so, share your knowledge with the class. 4) How did the Arab world do during the Middle Ages? 5) Make a list of the Arab world's achievements of that time. Comment on some of them. 6) How did other civilizations develop during the Middle Ages?

Exercise 3.

A. Read the text. Think of a good title.

In the Europe of Latin alphabet – from which modern cryptology would spring – cryptography flickered weakly. <…> A knowledge of it is requisite to an understanding of all subsequent techniques of substitution cryptanalysis.

(Compiled from *Kahn, D. The Codebreakers. The Story of Secret Writing. – New York: Macmillan Publishing Company, 1967. – 1164 p.*)

B. Divide the text into logical parts. Write an outline of the text.

C. Prepare to discuss in detail the facts given in the text. Look up any words that you may not know but you may need to discuss the text in class. Make sure you pronounce the words correctly.

Exercise4. Answer the questions.

1) What kind of change took place in Europe with the collapse of the Roman empire? How did it affect cryptology? How long did the period last? 2) What was Roger Bacon's contribution to cryptology? 3) What role did Geoffrey Chaucer play in the development of cryptography in the Middle Ages? Why are his encipherments referred to as *illustrious*? 4) How was cryptology perceived in the Middle Ages? Why so? Give examples. 5) Why was cryptology confused with the Jewish kabbalah? 6) What people is reputed to give birth to cryptology? 7) What brought about a break-through in cryptology? 8) What literary sources prove that cryptology was flourishing among the Arabs? 9) Where was the Arabic knowledge of cryptography fully set forth? What kind of work is it? What sections does it contain? 10) What was Qalqashandi famous for? What writings did he attribute most of his information on cryptology to? 11) What systems of cipher did Qalqashandi describe? What makes it unique? 12) What way of solving a message received in code did Ibn ad-Duraihim suggest? How did it affect subsequent techniques of substitution cryptanalysis?

Exercise 5. Write a summary of the above text.

Exercise 6. Refer to your outline of the text (Exercise 3(B)). For each point of the outline write out key words and word combinations that may come in handy in retelling the text. Prepare to comment on the facts and enlarge upon the topic.

Exercise7. Refer to your summaries / outlines of the four texts given in this unit (sections 1 – 4). Think of the four pieces as a coherent text. Write a one- / one-and-a-half-page conclusion to the overall text.

UNIT II

THE RISE OF THE WEST

Section 1

Exercise 1.

A. How are the following words formed? Can you guess what they mean? Make sure you pronounce the words correctly.

(a) A dispatch, a substitute, an impress, transfer (of sth), (an) elaborate (organization), to progress, to school (smb), to delegate, to war;

(b) Christendom, to cryptanalyze, nomenclator, paramountcy, secretaryship, likewise, indigenously;

(c) indiscriminately, undiluted, undated, preemimance;

(d) city-states, cipher-presentations, letter-frequency.

B. Explain the meaning of the following words. How do you think they may be used in the context of cryptology?

Epithet, homophone, polyphone, mnemonic.

Exercise 2. Answer the questions.

1) What period does the Renaissance embrace? What civilization does it characterize? 2) What is typical of the Renaissance? 3) What political changes in the life of Europe is it associated with? How do you think those changes influenced cryptology? 4) What is political cryptology? 5) What is the difference between a code and a cipher? 6) What is nomenclator?

Exercise 3.

A. Read the text. What is its topic? Think of a good title.

Western civilization began the use of political cryptology that it has continued uninterrupted to the present as it emerged from the feudalism of the Middle Ages. <…> But Matteo exercised great prudence in constructing ciphers intended for use in France, England, Venice, and Florence – states for whose cryptology he professed great admiration.

(Compiled from *Kahn, D. The Codebreakers. The Story of Secret Writing. – New York: Macmillan Publishing Company, 1967. – 1164 p.*)

B. Refer to Exercise 2. Did you manage to answer all the questions? If you failed to do so, try to find answers in the above text.

C. Divide the text into logical parts. Write an outline of the text.

D. Prepare to discuss in detail the facts given in the text. Look up any words that you may not know but you may need to discuss the text in class. Make sure you pronounce the words correctly.

Exercise4. Answer the questions.

1) What kind of cryptology emerged from the feudalism of the Middle Ages? Did it reflect the achievements of the previous epochs? 2) How did it develop thereafter? 3) What two basic modern

forms of secret writing existed from the earliest days? 4) What did the substitutions of code stem from? Give an example. 5) What facts prove that as early as 1226 a faint political cryptology appeared in the archives of Venice? 6) What earliest examples of the nomenclator are given in the text? What do you make of them? 7) How did the early nomenclators develop thorough the subsequent centuries? When and why were homophones introduced? What did they have to do with frequency analysis? 8) Where could that knowledge come from? Does the evidence given in the text seem convincing to you? 9) What facts testify that by the end of the 16th century cryptology had become really important? 10) How is Venice's cryptology characterized in the text? 11) What was the name of the West's first great cryptanalyst? Do his works on cryptology survive? 12) Was Venice the only locale of export of expert cryptanalysts during the Renaissance? 13) What were Pirrho Musefili and Cieco Simonetta famous for? Where did they work? 14) What contributions did France and England make to cryptology? 15) What kind of cryptologists worked in the service of the Supreme Pontiff? 16) What made the Argentis remarkable in the field of cryptology? Make a list of their innovations.

Exercise 5. Write a summary of the above text.

Exercise 6. Refer to your outline of the text (Exercise 3(C)). For each point of the outline write out key words and word combinations that may come in handy in retelling the text. Prepare to comment on the facts and enlarge upon the topic.

Section 2

Exercise 1. How are the following words formed? Can you guess what they mean? Make sure you pronounce the words correctly.

(a) The disuse, to dethrone, presumably, proliferation, unbreakable (cipher), watchfulness;

(b) to project (an image), to boomerang;

(c) archfoe, headsman.

Exercise 2. Answer the questions.

1) Which of the following words does not go with the rest? (*Huguenot, Protestant, Catholic, Henry VIII, Elizabeth I, Henry of Navarre*) 2) What was the religious situation like in the Europe of the 16th century? How did it affect international affairs? / affairs inside the countries of France, England, Spain? 3) Which country was considered the richest and mightiest nation during the Renaissance? Why so? How do you think its world supremacy affected the development of cryptology? 4) What was the status of the Netherlands at that time? 5) What do you know about the role of Elizabeth I in the history of England? When did she reign? What kind of person was she? 6) Who was the king of Spain then? 7) What king did France have at the end of the 16th century? Was he popular in the history of France? 8) What did Mary, Queen of Scots, have to do with the relations between England and Spain? 9) How did her plans become known? 10) What did her plotting eventually lead to?

Exercise 3.

A. Read the text. What is its topic?

During the Renaissance cryptology was widely used. <…> But there seems equally little doubt that cryptology hastened her unnatural end.

(Compiled from *Kahn, D. The Codebreakers. The Story of Secret Writing. – New York: Macmillan Publishing Company, 1967. – 1164 p.*)

B. Refer to Exercise 2. Did you manage to answer all the questions? If you failed to do so, try to find answers in the above text.

C. Divide the text into logical parts. Write an outline of the text.

D. Prepare to discuss the role of cryptology in the life of Europe's royalty during the Renaissance. Look up any words that you may not know but you may need to discuss the text in class. Make sure you pronounce the words correctly.

Exercise4. Answer the questions.

1) What was typical of the first cryptological systems used in Iberia in 1480s? 2) What nomenclator set the pattern for Spanish cryptology well into the 17th century? What did it comprise? 3) Which countries' cryptanalytic abilities 'had a pope' in the 16th century? What kind of relations did they have with Spain? 4) What contribution to cryptology did François Viète make? 5) What was Philip van Marnix famous for? How did 'his demonstration of the value of cryptanalysis set in motion a train of events that culminated on a headsman's block?' 6) What report gave England tangible evidence of Spain's aggressive intentions? 7) What role did Walsingham play in uncovering the plot? 8) What was the name of England's first great cryptanalyst? What made him famous? 9) What did the conspiracies result in? 10) Was that the triumph of cryptology or its complete and utter failure? Give your reasons.

Exercise 5. Write a summary of the above text.

Exercise 6. Refer to your outline of the text (Exercise 3(C)). For each point of the outline write out key words and word combinations that may come in handy in retelling the text. Prepare to comment on the facts and enlarge upon the topic.

Exercise7. Refer to your summaries / outlines of the two texts given in this unit (sections 1,2). Think of the two pieces as a coherent text. Write a one- / one-and-a-half-page conclusion to the overall text.

UNIT III

RUSSIAN CRYPTOLOGY

Section 1

Exercise 1.

A. How are the following words formed? Can you guess what they mean? Make sure you pronounce the words correctly.

(a) Denominator, numerator, meddler, inmate, intercommunication, officialdom, superincipherment, unconquerable, underlying (nomenclator);

(b) an intercept, a suspect, to light-finger, to muddy;

(c) anglophile, codegroup, seal-forger, telltale, tomblike.

Exercise 2. Answer the questions.

1) When do you think political cryptology appeared in Russia? Account for your opinion. 2) When is a nation usually in need of cryptology? Were there such times in the history of Russia? What are they? 3) What was the political situation like inside the Russia of the 19th century? What political forces do you think might be interested in cryptography? Why so? 4) Account for the results of World War I. Why was Russia a failure?

Exercise 3.

A. Read the text. Think of a good title.

Although secret writing appears in Russia in the simple substitutions of 12th and 13th-century manuscripts, akin to those of medieval France and Germany <…> Indeed, it may not be too much to claim that the establishment of Communist Power, perhaps the supreme fact of contemporary history, was made possible to a significant degree by the cryptanalysis of czarist secret communications.

(Compiled from *Kahn, D. The Codebreakers. The Story of Secret Writing. – New York: Macmillan Publishing Company, 1967. – 1164 p.*)

B. Refer to Exercise 2. Did you manage to answer all the questions? If you failed to do so, try to find answers in the above text.

C. Divide the text into logical parts. Write an outline of the text.

D. Prepare to discuss in detail the facts given in the text. Look up any words that you may not know but you may need to discuss the text in class. Make sure you pronounce the words correctly.

Exercise4. Answer the questions.

1) What is the oldest Russian solution that England's archives have? What does it prove, in the author's opinion? Does his point of view seem convincing to you? 2) How can those first ciphers be characterized? 3) How did the situation change in the reign of Peter's daughter, Elizabeth? 4) How did cryptography develop in the time of Catherine the Great? 5) When did black chambers come into operation in Russia? 6) What was the cryptologic situation like during Napoleon's invasion of Russia? 7) How did cryptanalysts function during the 19th century? 8) What was Zybine famous for? 9) What ciphers did the Russian underground use? 10) What kind of cryptanalytic service did the Foreign Ministry have then? 11) Why were the cryptanalytic attempts of the Ministry of War a failure before and during World War I?

Exercise 5. Write a summary of the above text.

Exercise 6. Refer to your outline of the text (Exercise 3(C)). For each point of the outline write out key words and word combinations that may come in handy in retelling the text. Prepare to comment on the facts and enlarge upon the topic.

Section 2

Exercise 1.

A. How are the following words formed? Can you guess what they mean? Make sure you pronounce the words correctly.

(a) To adjudge, counterespionage, to imperil, to ingrain, illegitimate, to jeopardize, multiplicity, Nazidom, to overrun, prearranged, presumably, reappear, receipt, transmission;

(b) a codename, dark-souled, information-rich, image-bearing, hollowed-out, medium-level, stalemate, radio-intelligence, rotor-type, top-notch, windfall;

(c) an offensive, to fire, a neutral, to rest (upon something), to well up, to wireless.

B. Which of the words below does not go with the rest?

Intelligence, perspicacity, reconnaissance, surveillance, monitoring.

Exercise 2. Answer the questions.

1) Have you read anything about the work of the Soviet Union's intelligence agents before and during World War II? That countries did they work in? How did they communicate with the Soviet Union's intelligence services? Were ciphers and codes in wide use then? 2) What made the fabulous 'Lucy' network in Switzerland, the Rote Kapelle in Germany and the Sorge ring in Japan so legendary? 3) How do you think cryptology developed during the Cold War?

Exercise 3.

A. Read the text. What is the author's attitude to the topic discussed? Prepare to prove your point of view.

The strides that the Russian Army had made in cryptology after the traumatic experiences of World War I were dramatized by an interchange of messages between incredulous Russian units at the very start of the Russian-German War. <…> it has beyond question rocketed Red accomplishments in this black art to Sputnik height.

(Compiled from *Kahn, D. The Codebreakers. The Story of Secret Writing. – New York: Macmillan Publishing Company, 1967. – 1164 p.*)

B. Refer to Exercise 2. Did you manage to answer all the questions? If you failed to do so, try to find answers in the above text.

C. Divide the text into logical parts. Write an outline of the text.

D. Prepare to discuss in detail the facts given in the text. Look up any words that you may not know but you may need to discuss the text in class. Make sure you pronounce the words correctly.

Exercise4. Answer the questions.

1) How did the Soviet Union's cryptology function during World War II? 2) How can German radio intelligence against the Soviet Union be characterized? Did it enjoy strategic success? Did it succeed tactically? 3) Did the situation change thoughout the war? 4) What does the opinion that 'the Red Army of World War II was vastly different from the Imperial Russian Army of 1914 – 17' rest on? How does the author of the text assess the statement? Does his assessment show his attitude to the

Soviet Union's success in World War II? 5) What other facts show the author's attitude to the events described in the text? 6) How does the author of the text comment on the opinion that 'Russia lost World War I in the ether and won World War II there'? Is his reasoning convincing to you? 7) What is one-time pad? When did the Soviet Union begin to practice it? What did it result in? 8) What cryptographic means contributed to the success of the fabulous 'Lucy' network in Switzerland, the Rote Kapelle in Germany and the Sorge ring in Japan so legendary? 9) How did Russia take her security after World War II? Give examples. 10) What cryptographic systems served the internal needs of secret communications within spy rings? Give an example. 11) When and where was the book that contains the piece we have read published? What were the relations between the Soviet Union and the West like then? 12) Analyze the final paragraph of the above piece. What do you think of the conclusion the author of the text made? Does it show the author's knowledge, understanding of and attitude to the topic? Does it show something else?

Exercise 5. Write a summary of the above text.

Exercise 6. Refer to your outline of the text (Exercise 3(C)). For each point of the outline write out key words and word combinations that may come in handy in retelling the text. Prepare to comment on the facts and enlarge upon the topic.

UNIT IV

THE ANATOMY OF CRYPTOLOGY

Exercise 1.

A. How are the following words formed? Can you guess what they mean? Make sure you pronounce the words correctly.

(a) Ambiguity, alternation, addition, subtraction, columnar, linear, denial, decipherable, deviation, distinguishable, disturbance, enlightening, eternally, fixity, frequency, fruitfulness, metaphorical, markedly, preconcerted, permutation, refutation, reasoning, statistician, theoretician, validate, verification;

(b) a constant, to flag (an error), a garble, to key, to mirror, to radio, to total, the general, the specific, the initiated;

(c) dot-and-dash, easy-to-identify, information-processing, lucky-break, off-set, photolithography, secrecy-transformation, servomechanism, special-case (solutions), shorthand, well-defined.

B. Which of the following is the general term?

(a) Addition and subtraction in finite rings, coordinate transformations of lattice points, linear algebraic transformations, permutations in the set of primary elements, secrecy transformations;

(b) alveolar, columnar, graphical, linear, non-linear;

(c) corollary, hypothesis, phenomenon, premise, refutation;

(d) economy, policy, reliability, rapidity, security.

C. Think of an antonym for each of the words below.

Addition, analysis, concrete, cryptography, deductive, empirical, finite, general, implicit, noumenon, a posteriori, refutation, a variable.

D. Think of a synonym for each of the words below.

To attack (a problem), occurrence, premise, to back up, redundancy.

Exercise 2. Answer the questions.

1) What is the difference between cryptology, cryptography and cryptanalysis? What branches of science do you think each of them is related to? 2) What does a scientific method of solving a problem (used especially in natural sciences) consist in? What are its steps? Do you think it is applicable to cryptology? 3) When did information theory appear? What problems does it deal with? Why do you think it may rank among the 'enduring great' theories of man? 4) What 'great' theories of the 20th century could have influenced the development of cryptology? Explain why.

Exercise 3.

A. Read the text. What is its topic?

Cryptography and cryptanalysis are sometimes called twin or reciprocal sciences <…> No method is acceptable that does not accede to the requirement, that does not provide for both a general system and specific keys.

(Compiled from *Kahn, D. The Codebreakers. The Story of Secret Writing. – New York: Macmillan Publishing Company, 1967. – 1164 p.*)

B. Refer to Exercise 2. Did you manage to answer all the questions? If you failed to do so, try to find answers in the above text.

C. Divide the text into logical parts. Write an outline of the text.

D. Prepare to discuss in detail the facts given in the text. Look up any words that you may not know but you may need to discuss the text in class. Make sure you pronounce the words correctly.

Exercise4. Answer the questions.

1) How do cryptography and cryptanalysis relate? 2) What makes them different? 3) Which of the two uses mathematical methods? What does it mean? 4) Which of the two relies on methods employed by physical sciences? What does it imply? 5) What distinction does philosophy offer in this respect? 6) Where does the empirical nature of cryptanalysis appear? 7) What is the common ground of scientific method between cryptanalysis and other sciences? 8) What are deductive solutions based on? Explain their mechanism. 9) What are inductive solutions based on? Explain their mechanism. 10) How did those solutions develop? 11) What is implied by *fixity of letter frequency*? Why is it important for cryptanalysis? What other activities depend on it? 12) How did the development of information theory affect cryptology? What new concepts were introduced? 13) What sources of redundancy are of particular importance for their role in determining the frequency table? Give an example of redundancy from ordinary language. 14) Why do people put in their own redundancy where the language has none? Give an example. 15) How does redundancy bring numerous cryptologic phenomena under a single broad generalization? Why are puzzle cryptograms harder to solve than ordinary messages? 16) How did Shannon view cryptology? 17) In what sense may cryptology be regarded as a conflict? 18) How do cryptology and sociology relate? 19) What requirements should all cryptosystems meet? Arrange them as a hierarchy.

Exercise 5. Write a summary of the above text.

Exercise 6. Refer to your outline of the text (Exercise 3(C)). For each

point of the outline write out key words and word

combinations that may come in handy in retelling the text.

Prepare to comment on the facts and enlarge upon the topic.

Exercise 7. Prepare to give a talk on the recent advances of cryptology.

ЛИТЕРАТУРА

1. *Вербицкий А. А.* Активное обучение в высшей школе: контекстный подход. – М.: Высшая школа, 1991. – 207 с.
2. *Яроцкая Л. В.* Информационная безопасность и защита информации: Учебное пособие для документоведов. – М.: МГЛУ, № Гос. регистр. 335, 2011. – 93 с.
3. *Яроцкая Л. В.* Обучение студентов нелингвистического профиля межкультурному общению в профессиональной среде // Современный образовательный контекст: традиции и инновации в обучении иностранным языкам: сб. научн. тр., Часть 1: Современные тенденции в обучении иностранным языкам студентов нелингвистических специальностей. – М.: ИПК МГЛУ «Рема», 2012. – С.110 –117.
4. *Яроцкая Л. В.* Профессионально ориентированный учебник английского языка для студентов-нефилологов // Актуальные проблемы профессионально-методической подготовки преподавателей иностранного языка. – М.: Рема, 2007. – С. 157–162. (Вестн. Моск. гос. лингв. ун-та; вып 516. Сер. Лингводидактика).
5. *Яроцкая Л. В. , Желнов И. И.* Реализация межкультурной парадигмы лингводидактики в предметном поле «Защита информации» (на примере специализированного учебного пособия) [Электронный ресурс] // Интернет-журнал «Науковедение». – 2013. – № 2 (15). – С. 48. – Режим доступа: http://naukovedenie.ru/PDF/41pvn213.pdf, свободный –Загл. с экрана. ISSN 2223–5167. Идентиф. номер статьи в журнале: 41ПВН213.
6. *Яроцкая Л. В., Титкова О. И., Смольянникова И. А., Желнов И. И.* Информационно-образовательный ресурс «Межкультурная профессиональная коммуникация» как современная образовательная технология: Коллективная монография [Электронный ресурс]. – М.: Мир науки, 2013. – 162 с.
7. *Яроцкая Л. В., Титкова О. И., Смольянникова И. А., Желнов И. И.* Концептуальные основы информационно-образовательного ресурса «Межкультурная профессиональная коммуникация» [Электронный ресурс] // Интернет-журнал «Науковедение». – 2013. – № 2 (15). – С. 49. – Режим доступа: http://naukovedenie.ru/PDF/42pvn213.pdf, свободный –Загл. с экрана. ISSN 2223–5167. Идентиф. номер статьи в журнале: 42ПВН213.

Ludmila Yarotskaya
Moscow State Linguistic University
Russia, Moscow
E-Mail: lvyar@yandex.ru

Ilia Zhelnov
Moscow State Linguistic University
Russia, Moscow
E-Mail: jelnov-i@yandex.ru

The problem of modelling sociocultural context in the field of "information security" revisited (with reference to a specialized foreign language manual)

Abstract: In the article, the authors sum up their experience of modelling sociocultural context employed to realize cross-cultural paradigm in teaching students majoring in the field of information security.

The authors substantiate as necessary a complex approach to working out new manuals meant to develop inter-cultural foreign language vocational communicative competence. The basic criterion for selecting texts is proved to be their polyperspective information potential – treatment of the regular processes and tendencies underlying the development of the science of information security since ancient times to the present day in the general historic, specific ethno-cultural, and subject-centered contexts.

Keywords: Information security; sociocultural context; inter-cultural foreign language vocational communicative competence; criteria for selecting texts; the polyperspective information potential of texts.

REFERENCES

1. Verbickij A. A. Aktivnoe obuchenie v vysshej shkole: kontekstnyj podhod. – M.: Vysshaja shkola, 1991. – 207 s.
2. Jarockaja L. V. Informacionnaja bezopasnost' i zashhita informacii: Uchebnoe posobie dlja dokumentovedov. – M.: MGLU, № Gos. registr. 335, 2011. – 93 s.
3. Jarockaja L. V. Obuchenie studentov nelingvisticheskogo profilja mezhkul'turnomu obshheniju v professional'noj srede // Sovremennyj obrazovatel'nyj kontekst: tradicii i innovacii v obuchenii inostrannym jazykam: sb. nauchn. tr., Chast' 1: Sovremennye tendencii v obuchenii inostrannym jazykam studentov nelingvisticheskih special'nostej. – M.: IPK MGLU «Rema», 2012. – S.110 –117.
4. Jarockaja L. V. Professional'no orientirovannyj uchebnik anglijskogo jazyka dlja studentov-nefilologov // Aktual'nye problemy professional'no-metodicheskoj podgotovki prepodavatelej inostrannogo jazyka. – M.: Rema, 2007. – S. 157–162. (Vestn. Mosk. gos. lingv. un-ta; vyp 516. Ser. Lingvodidaktika).
5. Jarockaja L. V. , Zhelnov I. I. Realizacija mezhkul'turnoj paradigmy lingvodidaktiki v predmetnom pole «Zashhita informacii» (na primere specializirovannogo uchebnogo posobija) [Jelektronnyj resurs] // Internet-zhurnal «Naukovedenie». – 2013. – № 2 (15). – S. 48. – Rezhim dostupa: http://naukovedenie.ru/PDF/41pvn213.pdf, svobodnyj –Zagl. s jekrana. ISSN 2223–5167. Identif. nomer stat'i v zhurnale: 41PVN213.
6. Jarockaja L. V., Titkova O. I., Smol'jannikova I. A., Zhelnov I. I. Informacionno-obrazovatel'nyj resurs «Mezhkul'turnaja professional'naja kommunikacija» kak sovremennaja obrazovatel'naja tehnologija: Kollektivnaja monografija [Jelektronnyj resurs]. – M.: Mir nauki, 2013. – 162 s.
7. Jarockaja L. V., Titkova O. I., Smol'jannikova I. A., Zhelnov I. I. Konceptual'nye osnovy informacionno-obrazovatel'nogo resursa «Mezhkul'turnaja professional'naja kommunikacija» [Jelektronnyj resurs] // Internet-zhurnal «Naukovedenie». – 2013. – № 2 (15). – S. 49. – Rezhim dostupa: http://naukovedenie.ru/PDF/42pvn213.pdf, svobodnyj –Zagl. s jekrana. ISSN 2223–5167. Identif. nomer stat'i v zhurnale: 42PVN213.