Л.К.Сальная

Secure IT

English for Information Protection Specialities

Л.К.Сальная

Secure IT

Учебное пособие

для студентов второго образовательного уровня

Таганрог 2019

ББК 81.2Англ
Secure IT: Учебное пособие / Сост. Л. К. Сальная – 203 с.
Под общей редакцией Г. А. Краснощековой

Учебное пособие Secure IT предназначено для студентов второго образовательного уровня (бакалавриат), а также может быть интересным в качестве дополнительного материала для магистрантов и аспирантов специальностей в области информационной безопасности.

В качестве учебного материала в пособии используются англоязычные тексты, взятые из оригинальных печатных и электронных источников, связанные с различными направлениями защиты информации. Учебное пособие предназначено для использования в учебном процессе при обучении студентов третьего и четвертого курсов специальностей в области информационной безопасности.

Материал учебного пособия направлен на формирование профессионально-ориентированной коммуникативной компетенции студентов по направлению их будущей деятельности в области информационной безопасности.

Структура учебного пособия сформирована в соответствии с поставленной задачей. Пособие содержит десять основных разделов (units), каждый из которых включает следующие подразделы: задания для тренировки произношения терминов (pronunciation), задания для ознакомления с лексикой раздела (memorize the terms), работа с аутентичными текстами (text 1), задания на закрепление лексики раздела (vocabulary tasks), тексты с заданиями на выборочное и просмотровое чтение (text 2), работа по систематизации и освоению той части английской грамматики, которая характерна для научно-технической литературы (grammar reference, grammar), а также разделы writing и communication, позволяющие студентам формировать навыки письменного и устного профессионально-ориентированного иноязычного общения в наиболее типичных ситуациях.

Учебное пособие предназначено для аудиторной и внеаудиторной (групповой и индивидуальной) работы. Каждый из основных разделов пособия (unit), содержит учебный текст для аудиторной работы с предтекстовыми заданиями, вопросами и лексическими заданиями разного уровня сложности, в том числе и заданиями на перевод с английского языка на русский и с русского языка на английский. Работа с грамматикой в пособии начинается с установления уровня сформированности лингвистической компетенции при помощи тестов остаточных знаний трех уровней сложности в подразделе грамматики первого раздела (Unit 1. Grammar tasks. Revision. Check your grammar.). Грамматический минимум пособия охватывает основной грамматический материал, касающийся особенностей научно-технической литературы, и содержит упражнения различного уровня сложности (A, B, C). В пособии также представлены задания на повторение и обобщение пройденного материала (Vocabulary and Grammar 1-6. Revision. Vocabulary and Grammar 7-10. Revision).

Подразделы Communication и Writing предлагают студентам раскрыть различные аспекты тематики раздела, подготовить и обсудить доклады, презентации, проектные задания, а также научиться составлять резюме, краткое жизнеописание, необходимые в процессе поиска работы, выделить свои сильные стороны на собеседовании.

В целом, задания направлены на формирование профессионально-ориентированной коммуникативной компетенции студентов в сфере будущей профессиональной деятельности и

готовят студентов к профессионально-ориентированному иноязычному общению: поиску работы, интервью, общению с коллегами, партнерами, деловым поездкам.

Все англоязычные тексты, используемые в пособии, взяты из оригинальной литературы: стандартов, научных статей, руководств пользователя информационными системами. Они сокращены, но не адаптированы. Разноуровневые упражнения к текстам направлены на формирование умений ознакомительного и изучающего чтения, а также профессионально-ориентированной коммуникативной компетенции. Основные темы текстов, которые представлены в пособии, это – методы и средства обеспечения безопасности информационных технологий, критерии оценки безопасности, в части функциональных требований и требований доверия, анализ рисков и управление безопасностью, криптографические методы и методы криптоанализа, способы и методы защиты информации в глобальных сетях и интрасетях.

Contents

Unit 1. COMMON CRITERIA SECURITY EVALUATION. ……..…..8
Unit 2. COST/BENEFIT ANALYSIS OF THE RISK. …….. 24
Unit 3. METHODS OF CRYPTOGRAPHY. ……. 41
Unit 4. MODERN METHODS OF CRYPTANALYSIS. ……..…. 58
Unit 5. STEGANOGRAPHY. …… 75
Unit 6. QUANTUM CRYPTOGRAPHY …….. 91
Vocabulary and Grammar 1-6. Revision. ……..…..… 101
Unit 7. MEANS AND METHODS FOR THE INFORMATION
PROTECTION IN THE INTERNET …….....… 107
Unit 8. INTRANET SECURITY ……..... 121
Unit 9. FIREWALL ……..…. 136
Unit 10. WIRELESS COMMUNICATION ……..… 149
Vocabulary and Grammar 7-10. Revision. ……...…..... 160
Appendix 1. Grammar reference ……..…….. 167
Appendix 2 ……..…… 177
Appendix 3 ……..…… 179
Appendix 4 ……..… 182
Appendix 5 ……..… 184
Word List ..……...…… 187

UNIT 1. COMMON CRITERIA SECURITY EVALUATION

Pronunciation

Make sure you pronounce the following words properly:

availability [ə˛veɪlə'bɪlɪtɪ]	unauthorized [ʌn'ɔ:θəraɪzd]
threat [θret]	disclosure [dɪs'kləuʒə]
procurement [prə'kjuəmənt]	malicious [mə'lɪʃəs]
assurance [ə'ʃuərəns]	target ['tɑ:gɪt]
criterion [kraɪ'tɪərɪən]	applicable ['æplɪkəbl]

Memorize the terms

1. Read the following terms and their definitions and memorize them:

availability – the protection of IT products so that they can be used by the intended user only

confidentiality – a category of information protection that involves measures to keep the information secret and secure it from unauthorized disclosure

implement – carry into effect, bring into action, perform

malicious – evil-minded, having some evil purpose, e.g. a malicious act

procurement – purchase

software – programs that give instructions to the computer hardware and control its work

threat – an act that can cause the breakdown of information protection system, e.g. threat of unauthorized disclosure

tolerable – acceptable, receivable, e.g. tolerable risk

unauthorized disclosure – an access to IT products or systems performed by a person who doesn't have rights to do it

2. Match the following words with their Russian equivalents:

firmware	скрытый, неявный
assurance measures	соответствие, согласованность
security risk	реализация
integrity	риск нарушения информационной безопасности
implementation	целостность
conformance	программно-аппаратное обеспечение, встроенные программы
implicit	средства обеспечения доверия

3. Match the following words with their synonyms:

evaluation	(security) task
meet the requirements	breaking a security system
have an impact	control
consumer	assessment
(security) target	user
oversight	influence
failure of security	satisfy demands

Reading

4. Pre-reading task.

What sort of information should be protected? What measures can be taken to protect information? What do you know about Common Criteria

Security Evaluation? Comment on the phrase “People who have information rule the world”.

5. Read the text and find the information about the purpose of creating the standard and who it was established for.

Text 1. Common criteria security evaluation.

The Common Criteria (CC) is meant to be used as the basis for evaluation of security properties of IT products and systems. By establishing such a common criteria base, the results of an IT security evaluation will be meaningful to a wider audience.

The CC will permit comparability between the results of independent security evaluations. It does so by providing a common set of requirements for the security functions of IT products and systems and for assurance measures applied to them during a security evaluation. The evaluation process establishes a level of confidence that the security functions of such products and systems and the assurance measures applied to them meet these requirements. The evaluation results may help consumers to determine whether the IT product or system is secure enough for their intended application and whether the security risks implicit in its use are tolerable.

The CC is useful as a guide for the development of products or systems with IT security functions and for the procurement of commercial products and systems with such functions. During evaluation, such an IT product or system is known as a Target of Evaluation (TOE). Such TOEs

include, for example, operating systems, computer networks, distributed systems, and applications.

The CC addresses protection of information from unauthorized disclosure, modification, or loss of use. The categories of protection relating to these three types of failure of security are commonly called confidentiality, integrity, and availability, respectively. The CC may also be applicable to aspects of IT security outside of these three. The CC concentrates on threats to that information arising from human activities, whether malicious or otherwise, but may be applicable to some non-human threats as well. In addition, the CC may be applied in other areas of IT, but makes no claim of competence outside the strict domain of IT security.

The CC is applicable to IT security measures implemented in hardware, firmware or software. Where particular aspects of evaluation are intended only to apply to certain methods of implementation, this will be indicated within the relevant criteria statements.

6. Answer the following questions.

What is the purpose of creating this standard?

What is the sphere of CC application?

What is meant by TOE?

How do parties use the standard?

What are the main types of security failure?

What are the categories of protection related to them?

7. Mark the following statements true or false. Correct the false statements.

1. Common Criteria is created as a common set of requirements for developing IT products and systems.

2. Consumers of IT products and system can use this standard while assessing the security of their purchase.

3. During evaluation, an IT product or system is known as a Security Target of Evaluation.

4. Integrity is the category of information protection relating to the failure of security called unauthorized disclosure.

5. The CC is used to IT security measures implemented in software.

6. The CC concentrates on malicious human threats.

7. This standard is possible to use in any IT sphere.

Vocabulary tasks

8. Form the word combinations and give their definitions.

Security, protection, evaluation.

9. Complete the sentences using the words given below.

Require, judgments, inspection, certification, a set.

1. The certification process is the independent _____ of the results of the evaluation leading to the production of the final certificate or approval.
2. The CC is presented as _____ of distinct but related parts.
3. The evaluation scheme, methodology and _____ processes are the responsibility of evaluation authorities that run evaluation scheme.
4. Many of the evaluation criteria _____ the application of expert judgments and background knowledge for which consistency is more difficult to achieve.

5. The CC contains criteria to be used by evaluators when forming _____ about the conformance of TOEs to the security requirements.

10. Make the word combinations.

1. distributed	a) profile
2. fulfill	b) comparability
3. make	c) disclosure
4. permit	d) the requirements
5. loss	e) measures
6. security	f) claims
7. protection	g) of use
8. assurance	h) system
9. unauthorized	i) function
10. meet	j) the needs

11. Match the term and its definition.

1. Evaluation authority
2. Target of Evaluation
3. Assets
4. Augmentation
5. Protection Profile

a) information or resources to be protected by the countermeasures of a TOE.

b) the addition of one or more assurance components from Part 3 to an EAL or assurance package.

c) a body that implements the CC for a specific community by means of evaluation scheme and thereby sets the standards and monitors the quality of evaluation.

d) an implementation-independent set of security requirements for a category of TOEs that meets specific consumer needs.

e) an IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

12. Complete the text by translating Russian phrases given in brackets.

Information held by (1 продукты и системы информационных технологий) is a critical resource that enables organisations to succeed in their mission. Additionally, individuals have a reasonable expectation that their (2 частная информация, содержащая) IT products or systems remains private, be available to them as needed, and not be subject to (3 несанкционированных изменений). IT products or systems (4 должны выполнять свои функции) while exercising proper control of the information to ensure that it (5 защищена от опасности) such as (6 нежелательного или незаконного распространения, изменения или потери). The term IT security is used to cover prevention and mitigation of these and similar hazards.

Many consumers of IT (7 не хватает знаний, компетенции или средств) necessary to judge whether their confidence in the security of their IT products or systems is appropriate, and they (8 могут не захотеть полагаться только на заверения разработчиков).

Consumers may therefore choose to increase their confidence in the security measures of an IT product or system by ordering (9 оценка безопасности).

The CC can be used to select the appropriate IT security measures and it contains criteria for evaluation (10 требований безопасности).

13. Read the second part of the text. Name the topics which are outside the scope of CC.

Text 2.

Certain topics, because they involve specialised techniques or because they are somewhat peripheral to IT security, are considered to be outside the scope of the CC. Some of these are identified below.

a) The CC does not contain security evaluation criteria pertaining to administrative security measures not related directly to the IT security measures. However, it is recognised that a significant part of the security of a TOE can often be achieved through administrative measures such as organisational, personnel, physical, and procedural controls. Administrative security measures in the operating environment of the TOE are treated as secure usage assumptions where these have an impact on the ability of the IT security measures to counter the identified threats.

b) The evaluation of technical physical aspects of IT security such as electromagnetic emanation control is not specifically covered, although many of the concepts addressed will be applicable to that area. In particular, the CC addresses some aspects of physical protection of the TOE.

c) The CC addresses neither the evaluation methodology nor the administrative and legal framework under which the criteria may be

applied by evaluation authorities. However, it is expected that the CC will be used for evaluation purposes in the context of such a framework and such a methodology.

d) The procedures for use of evaluation results in product or system accreditation are outside the scope of the CC. Product or system accreditation is the administrative process whereby authority is granted for the operation of an IT product or system in its full operational environment.

Evaluation focuses on the IT security parts of the product or system and those parts of the operational environment that may directly affect the secure use of IT elements. The results of the evaluation process are consequently a valuable input to the accreditation process. However, as other techniques are more appropriate for the assessments of non-IT related product or system security properties and their relationship to the IT security parts, accreditors should make separate provision for those aspects.

e) The subject of criteria for the assessment of the inherent qualities of cryptographic algorithms is not covered in the CC. Should independent assessment of mathematical properties of cryptography embedded in a TOE be required, the evaluation scheme under which the CC is applied must make provision for such assessments.

14. Grammar tasks. Revision. Check your grammar.

Task A.

I. Choose the correct form of the verb.

1. Usually I *have/am having* breakfast at 8.

2. Look! What *are the children doing/do the children do*?

3. Hello! I *haven't seen/didn't see* you for ages.

4. Tom *has met/met* his friends yesterday.

5. When I *last have seen /saw* her, she *went/ was going* to Moscow.

6. *Have you read/did you read* all these books? – I *have read/read* them last month.

7. I *have lost /lost* my notebook. *Have you seen/Did you see* it anywhere?

8. If we *go/will go* shopping, we *buy/will buy* something tasty.

9. He is so annoyed. If he *leave/left* earlier, he *will catch /would catch* the train.

10. I *have redecorated/have been redecorating* my sitting-room.

It'll be ready next week.

11. When I *went/came* home, my mother already *cooked/had* already *cooked* dinner.

II. Choose the correct modal verb.

1. I *can/have to* start my work early in the morning.

You *must /should* get up early, I think.

2. He *can/may* swim and play tennis.

3. You *can/may* come in and sit down.

4. The train *has to be/might be* late. It depends on the weather.

5. You *can/must* come and see us! We'll be happy to see you.

6. I *should/have to* learn English for my university exam.

7. I *might not/can't* talk to my friends' parents. I don't speak French.

III. Choose the correct form.

1. I like *to watch/watching* football very much.

2. We'd like *to buy/buying* a tour to New Zealand.

3. I hope *to pass/pass* my driving test.

4. Old comedies always make me *to laugh/laugh*.

5. My sister hates *read/reading* detective stories.

6. We went to the hospital *to visit/visit* our aunt. She was glad *to see/seeing* us.

7. We couldn't stop *to talk/talking* to her.

IV. Choose the correct form of the verb in Active or Passive Voice.

1. The roof of the house *broke/was broken* by the storm.

2. *Have you booked/have you been booked* the tickets?

3. Rubens *painted/was painted* his "perfect" ladies in the seventeenth century.

4. Thieves *stole/were stolen* a world-famous painting last night.

5. German and English *speak/are spoken* here.

6. This book *will publish/will be published* next month.

7. He *hasn't seen/hasn't been seen* anywhere.

8. The student *is listening/is being listened* now.

V. Choose the correct preposition.

1. She has always been interested *at/on/in* Maths.

2. He is good *at/on/in* English.

3. Have you ever been *at/on/to* London?

4. The conference starts *at/on/in* Monday.

5. They will come *at/on/in* the evening.

6. Usually they come *at/on/in* 7.

7. The laboratory is situated *at/in/of* the center *at/in/of* the town.

VI. Put an article or an expression of quantity where necessary.

1. *A/the/*– longest mountain range in *a/the/*– world is *a/the/* – Andes in *a/the/*–

South America.

2. Would you like *a/the/some* coffee? – I'd prefer *a/the/some* glass of *a/the/–* juice.

3. There is *a lot of/many/much* pollution in this region.

4. Nick lives far from *a/the/–* city center. There isn't *a lot of/many/much* noise.

5. She's made *a lot of/a few/a little* mistakes. Just one or two.

6. How *many/much/a lot of* work have you written? – Just *a lot of/a few/a little.*

7. He lives in *a/the/* – Cowan street. He goes to *a/the/* – work by *a/the/–* bus.

VII. Choose the correct form of an adjective or an adverb.

1. He is *old/older/ the oldest* than he looks.

2. She is as *bright/brighter/the brightest* as her sister.

3. It's *the high/the most high/the highest* mountain.

4. You live *far/farer/farther* than me.

5. It's *crowdeder/more crowded/the most crowded* street than that one.

6. It's *the comfortablest/the more comfortable/ the most comfortable* hotel in the town.

7. You've made *the bad/the baddest/the worst* report I've ever heard.

8. *Beautiful/more beautiful/the most beautiful* pictures make you feel fine.

Task B.

I. Put the verbs in the correct form. Present Simple, Present Continuous,

Present Perfect.

1. All people in Australia (share) its national passion – surfing.

2. We (go) to my sister's wedding next month.

3. What you (be) busy with? – I just (write) the report and now I (read) my e-mail.

4. What she (do)? – She (be) an artist. She just (finish) the college and (think) of changing the place of work now.

5. You still (cook)? – No, I already (cook) dinner.

6. I (envy) you. You (cook) so quickly.

7. Where you (go)? – We (go) for a run.

8. When I (go) home, I (take) you.

II. Put the verbs in the correct form. Past Simple, Past Continuous, Past Perfect, Future–in–the Past.

1. What the first vending machine (sell)?

2. If he (win) 1000$, he (buy) a beautiful yacht.

3. When we (arrive) at the party, Laura already (leave).

4. When Sarah (come) home, her mother (cook) dinner and (ask) Sarah to help her.

5. If I (be) the president of my country, I (support) the development of high technologies.

6. When Tim (come) to the airport, he (remember) that he (forget) his documents.

7. When I (drive) home, I (see) an accident.

III. Fill in the gaps using articles where necessary.

1. I want to become ____ manager.

2. We'll be there in ____ couple of hours.

3. She goes to the university by ____ train.

4. This lake is in ____ United States.

5. ____ river Rhine flows through ____ Switzerland.

6. ____ Kiev is ____ capital of ____ Ukraine.

7. She lives in ____ city centre.

IV. Put the verbs in brackets in the correct form. Infinitive, to – infinitive, Gerund.

1. I don't really like (sunbathe).
2. The doctor told me (do) more exercises.
3. I hate (get stuck) in traffic jam.
4. The film made me (laugh).
5. He really enjoys (buy) presents. When he starts (go) round the souvenir shops, it's difficult for him (stop).
6. Let me (think). I'd like (be left) alone.
7. We went to Moscow (enter) the university.

V. Put adjectives and adverbs in the correct degree of comparison.

1. James Bond is considered to be (brave) and (attractive) men in the world.
2. My brother is as (tall) as me.
3. Anna is (old) than she looks.
4. The test is (complicated) than it seems.
5. My brothers are very (pale). They have (strong) legs and can run (quickly).
6. Democracy is (bad) form of government from all the others.
7. All animals are equal, but some animals are (equal) than others.

VI. Fill in the gaps using prepositions where necessary.

1. They arrived ____ the station ____ 8.00.

2. What have we got ____ dinner? – Don't worry ____ it. Your favorite lamb will be ready ____ 20 minutes.

3. ____ last year we were ____ holiday ____ Egypt.

4. I'm so tired ____ housework!

5. ____ Monday morning we have Maths.

Task C.

I. Put the verbs in the correct form.

1. If I (have) more free time, I (go) jogging every day, but I (be) too busy recently that I (quit) even (do) morning exercises.

2. He (love) (dance) and (hope) (become) a professional dancer one day. He (go) (dance) for 7 years and (win) 3 awards since then. He (like) (found) his dancing school when he (be) 30.

3. Jane (be) so nervous these days – she (try) (find) a job. She (see) the manager of BP tomorrow morning. – I'm sure, if she (want), she (get) the job she (like).

4. My room (decorate) now. It (finish) in two weeks. The walls already (paint).

II. Put the articles and the expressions of quantity where necessary.

1. Where is ___ coffee? – It's in ___ cupboard on ___ left.

2. There are ___ pubs in ___ north of ___ Britain.

3. We need ___ eggs, ___ flour, ___ milk. We're going to bake ___ cake.

III. Put the adjectives and adverbs in the correct degree of comparison.

1. (large) animal that ever walked the planet was (tall) that giraffe and (heavy) than five elephants.

2. They were vegetarians and used their (long) necks to eat leaves from the tops of the trees.

3. They were as (calm) as all vegetarians and considered to be (ancient) creatures that lived on the Earth.

IV. Put prepositions where necessary.

1. He suffers ____ headaches.

2. ____ Christmas morning children wait for presents.

3. This bag is similar ____ mine.

4. I'm afraid ____ spiders.

5. He broke the pen ____ accident.

15. Communication.

Discuss your plans for the course. Distinguish the sphere of your scientific and professional interests, present and discuss it with your group-mates.

Questions for the discussion.

What do you know about the early days of information protection?

What are the main spheres of information protection?

Which sciences are closely connected with the areas of information protection?

Which companies are the leaders in the development of information protection means? Which Russian companies take leading positions at the market of information protection means?

Unit 2. COST/BENEFIT ANALYSIS OF THE RISK

Pronunciation

Make sure you pronounce the following words properly:

estimate ['estɪmət]	asset ['æset]
evaluate [ɪ'vælјueɪt]	severe [sɪ'vɪə]
unacceptable [ʌnək'septəbl]	environmental [ɪnvaɪərən'mentl]
consequence ['kɔnsɪkwəns]	sequence ['si:kwəns]
facility [fə'sɪlɪtɪ]	adversary ['ædvəsərɪ]
marginal ['mɑ:dʒɪnəl]	negligible ['neglɪdʒəbl]
minor ['maɪnə]	major ['meɪdʒə]
event [ɪ'vent]	vulnerable ['vʌlnərəbl]

Memorize the terms

1. Read the following terms and their definitions and memorize them:

access point – entry point into a computer or a program of the computer, entrance places of a facility (doors, windows etc.)

environmental impact statement – document that contains the results of the analysis of ecological effect

estimate risk – assess the risk of breaking the security system

facility – building, construction, machine, device or work tool

respective critical asset – resources, capital, facilities or information that might be used illegally

unacceptable risk – risk that can result in too high loss or damage of the information system or/of the enterprise under protection

undesired event – act or incident that can have negative results

2. Match the following words with their Russian equivalents:

fault tree	физическая безопасность
equation	обнаружить злоумышленника
law enforcement	исследование территории
consequence	диаграмма всех возможных последствий несрабатывания или аварии системы
site survey	принудительное осуществление закона
detect an adversary	уравнение, равенство
physical security	результат, последствия

3. Match the following words with their synonyms:

facility design blueprint	diminish, decrease
vulnerability	perform, execute
delay (an adversary)	estimate, evaluate
reduce (risk)	negative
assess	tolerable
acceptable	stop, capture
adverse	heliographic print, blue copy of a facility
commit (an act/event)	insecurity, weak point

Reading

4. Pre-reading task.

What measures can be used to persuade the managers to use security system?

What should be done to keep the high level of an enterprise security?

5. Scan the text and match the headings with its parts.

a. Identification of critical components.

b. Assessment of the physical protection systems vulnerability for facilities.

c. Risk assessment methodology.

d. Estimation of the relative consequence values.

e. Components of the facility characterization.

f. Initial steps in security system analysis.

Text 1. Cost/Benefit Analysis of the Risk.

__ Violence, vandalism, and terrorism are prevalent in the world today. Managers and decision-makers must have a reliable way of estimating risk to help them decide how much security is needed at their facility. A risk assessment methodology (RAM) has been refined by Sandia National Laboratories to assess risk at various types of facilities including US Mints and federal dams. The methodology is based on the traditional risk equation:

Risk = PA * (1 - PE) * C, where

PA is the likelihood of adversary attack,

PE is security system effectiveness,

1 - PE is adversary success, and

C is consequence of loss to the attack.

__ The process begins with a characterization of the facility including identification of the undesired events and the respective critical assets. Guidance for defining a design basis threat is included, as well as

for using the definition of the threat to estimate the likelihood of adversary attack at a specific facility. Relative values of consequence are estimated. Methods are also included for estimating the effectiveness of the security system against the adversary attack. Finally, risk is calculated. In the event, that the value of risk is deemed to be unacceptable (too high), the methodology addresses a process for identifying and evaluating security system upgrades in order to reduce risk.

__ An analysis methodology has been used to assess the vulnerability of physical protection systems for facilities. Here we describe the order and sequence of the seven basic steps of the methodology.

1. Characterize Facility

2. Identify Undesirable Events & Critical Assets

3. Determine Consequences

4. Define Threats

5. Analyze Protection System Effectiveness

6. Upgrade the System

7. Estimate Risks

Are Risks Acceptable? No / Yes

__ An initial step in security system analysis is **to characterize the facility operating states and conditions**. This step requires developing a thorough description of the facility itself (the location of the site boundary, building locations, floor plans, and access points). A description of the processes within the facility is also required, as well as identification of any existing physical protection features. This information can be obtained from several sources, including facility design blueprints, process

descriptions, safety analysis reports, environmental impact statements, and site surveys.

Undesired Events. The undesired events must be established. Undesired events are site-specific and have adverse impacts on public health and safety, the environment, assets, mission, and publicity.

Critical Assets. The adversary could cause each undesired event to occur in several ways. A structured approach is needed to identify critical components for prevention of the undesired events.

__ A logic model, like a fault tree, can be used to identify the critical components. The critical components and their locations become the critical assets to protect. There is the top-level portion of a generic fault tree for facilities.

Disrupt Mission of a Facility

1. Disruption of Operations
2. Crime Against Person(s)
3. Negative Publicity or Embarrassment
4. Theft of Assets
5. Destruction of Property

The next step is to categorize undesired events or loss of critical assets. The proposed categories of consequences are similar to those used by the Department of Defense per Military Standard 882C.

__ The consequence values and categories are described below. The goal is to estimate the relative consequence value associated with each undesired event.

Consequence Category	**Consequence Value**
Catastrophic	Very high

(results in death(s), total mission loss, or severe environmental damage)	
Critical *(results in severe injury/illness, major mission loss, or major environmental damage)*	High
Marginal *(results in minor injury/illness, minor mission loss, or minor environmental damage)*	Medium
Negligible *(results in less than minor injury/illness, less than minor mission loss, or less than minor environmental damage)*	Low

6. Answer the following questions

What are the first steps of the cost/benefit risk analysis?

Where can the information for the description of the facility be found?

What is a generic fault tree made for?

What are the kinds of a facility disrupt mission?

What should be done if the risk is estimated as unacceptable?

What are the results of undesired events?

Which documents are mentioned in the text?

What were these documents developed for?

7. Mark the following statements "true" or "false". Correct the false statements

1. PE is the likelihood of adversary attack.

2. Characteristic of the facility operating states and conditions requires a thorough description of the facility itself (the location of the site boundary, building locations, floor plans, and access points).

3. The consequence values are the critical assets to protect.

4. A logic model can be used to identify the critical components.

5. 1 - PE is adversary success.

6. Identification of any existing physical protection features can be obtained from a fault tree.

7. Cost / benefit analysis of the risk is needed to assure the consumer in the necessity of installing a protection system.

8. If the risk is assessed as unacceptable the protection system should be upgraded.

9. Destruction of property is categorized as the main critical component.

Vocabulary tasks

8. Form different parts of speech.

Verb	**Noun**
assess	
	evaluation
occur	
	threat
	category
characterize	

define	

9. Give your definitions of the following terms.

Estimate risk, facility, consequence, reduce risk, access point, severe environmental damage, threat.

10. Make the word combinations

1. site	a) detection
2. commit	b) definition
3. detect	c) operandi
4. protection	d) control
5. intrusion	e) boundary
6. threat	f) an adversary
7. assess	g) description
8. entry	h) an act
9. consequence	i) objective
10. modus	j) risk

11. What do the following abbreviations from Text 1 mean?

RAM, PA, PE, C

12. Complete the text using the words given below.

Events, weapons, to estimate, use, threat

Threat Definition. Before a vulnerability analysis can be completed, a description of the 1) … is required. This description includes the type of adversary, tactics, and capabilities (number in the group, 2) … , equipment, and transportation mode). Also, information is needed about the threat 3) … the likelihood that they might attempt the undesired 4) … . The specific type of threat to a facility is referred to as the design basis threat (DBT). The DBT is often reduced to several paragraphs that describe the number of adversaries, their modus operandi, the type of tools and weapons they would 5) … , and the type of events or acts they are willing to commit.

13. Translate into Russian the following paragraph.

Methods of detection include a wide range of technologies and personnel. Entry control, a means of allowing entry of authorized personnel and detecting the attempted entry of unauthorized personnel and contraband, is included in the detection function of physical protection. Entry control, in that it includes locks, may also be considered a delay factor (after detection) in some cases. Searching for metal (possible weapons or tools) and explosives (possible bombs or breaching charges) is required for high-security areas. This may be accomplished using metal detectors, x-ray (for

packages), and explosive detectors. Security police or other personnel also can accomplish detection. Security police or other personnel can contribute to detection if they are trained in security concerns and have a means to alert the security force in the event of a problem. An effective assessment system provides two types of information associated with detection: (1) information about whether the alarm is a valid alarm or a nuisance alarm, and (2) details about the cause of the alarm, i.e., what, who, where, and how many. The effectiveness of the detection function is measured by the probability of sensing adversary action and the time required for reporting and assessing the alarm.

14. Complete the text by translating Russian phrases given in brackets.

Establish Information Risk Management (IRM) Policy. A sound IRM program is founded on (1 хорошо продуманной инфраструктре IRM) that effectively addresses all elements of information security. (2 Общепринятые принципы информационной безопасности) currently being developed based on an Authoritative Foundation of supporting documents and guidelines will be helpful (3 в выполнении этого задания). IRM policy should begin with a high-level policy statement and supporting (4 цели), scope, constraints, responsibilities, and approach. This high-level policy statement should drive subordinate controls policy, (5 от логического управления доступа) to facilities security, (6 до прогноза внештатных ситуаций). Finally, IRM policy should be effectively communicated and enforced to all parties. Note that this is important both for (7 внутреннего контроля) and, with EDI,

the Internet, and other (8 внешние воздействия), for secure interface with the rest of the world.

15. Translate into English.

Специалист, несущий ответственность за выполнение заданий по оценке риска должен ясно представлять области, которые охватывает информационная безопасность.

Термин «угроза» обозначает события, которые могут иметь неблагоприятные последствия.

Управление информационными рисками – сложный процесс, требующий постоянного анализа рисков.

Вопросы безопасности должны быть неотъемлемой частью разработки компьютерных приложений.

Хорошо спланированная и выполненная оценка риска должна эффективно определять и измерять последствия широкого спектра угроз.

Количественная и качественная метрические схемы, применяемые для измерения элементов риска, были впервые разработаны Национальным бюро стандартов.

16. Read the second part of the text, write out key words and write down short definitions of the clue terms given in the text.

Text 2.

Threat Definition. Before a vulnerability analysis can be completed, a description of the threat is required. This description includes the type of adversary, tactics, and capabilities (number in the group, weapons, equipment, and transportation mode). Also, information is needed about the threat to estimate the likelihood that they might attempt

the undesired events. The specific type of threat to a facility is referred to as the design basis threat (DBT). The DBT is often reduced to several paragraphs that describe the number of adversaries, their modus operandi, the type of tools and weapons they would use, and the type of events or acts they are willing to commit.

The types of organizations that may be contacted during the development of a DBT description include local, state, and federal law enforcement (to include searching source material) and related intelligence agencies.

After the threat spectrum has been described, the information can be used together with statistics of past events and site-specific perception to categorize threats in terms of likelihood that each type of threat would attempt an undesired event. The likelihood of adversary attack can be estimated with a qualitative relative threat potential parameter. Below we describe the factors that can be used to estimate relative threat potential.

Adversary Capability

•Access to region

•Material resources

•Technical skills

•Planning/organizational skills

•Financial resources

Adversary History/Intent

•Historic interest

•Historic attacks

•Current interest in site

•Current surveillance

•Documented threats

Relative Attractiveness of Asset to Adversary

•Desired level of consequence

•Ideology

•Ease of attack

The process for estimating the threat potential follows a complete threat analysis and the parameter is estimated per undesired event and per adversary group. The basis of the parameter estimation includes:

• Characteristics of the adversary group relative to the asset to be protected

• Relative attractiveness of the asset to the adversary group.

The physical protection features must be described in detail before the security system effectiveness can be evaluated. An effective security system must be able to detect the adversary early and delay the adversary long enough for the security response force to arrive and neutralize the adversary before the mission is accomplished.

DETECTION, the first required function of a security system, is the discovery of adversary action and includes sensing covert or overt actions. In order to discover an adversary action, the following events must occur:

• sensor (equipment or personnel) reacts to an abnormal occurrence and initiates an alarm

• information from the sensor and assessment subsystems is reported and displayed

• someone assesses information and determines the alarm to be valid or invalid.

DELAY is the second required function of a security system. It impedes adversary progress. Delay can be accomplished by fixed or active

barriers, (e.g., doors, vaults, locks) or by sensor-activated barriers, e.g., dispensed liquids, foams. The security police force can be considered an element of delay if personnel are in fixed and well-protected positions.

RESPONSE, the third requirement of security systems, comprises actions taken by the security police force (police force or law enforcement officers) to prevent adversarial success. Response consists of interruption and neutralization. Interruption is defined as the response force arriving at the appropriate location to stop the adversary's progress. It includes the communication to the response force of accurate information about adversarial actions and the deployment of the response force. Neutralization is the act of stopping the adversary before the goal is accomplished. The effectiveness measures for neutralization are security police force equipment, training, tactics, and cover capabilities.

Protection System Effectiveness. Analysis and evaluation of the security system begin with a review and thorough understanding of the protection objectives and security environment. Analysis can be performed by simply checking for required features of a security system, such as intrusion detection, entry control, access delay, response communications, and a response force.

Risk Estimation

Risk is quantified by the following equation:

R = PA * (1-PE) * C

where R = risk associated with adversary attack

PA = likelihood of the attack

PE = likelihood that the security system is effective against the attack

(1 – PE) = likelihood that the adversary attack is successful (also the likelihood that security system is not effective against the attack)

C = consequence of the loss from the attack.

Upgrades and Impacts

If the estimated risk for the threat spectrum is judged to be unacceptable, upgrades to the system may be considered. The first step is to review all assumptions that were made that affect risk. All assumptions concerning undesired events, target identification, consequence definition, threat description, estimation of likelihood of attack, and safeguards functions should be carefully reevaluated. Upgrades to the system might include retrofits, additional safeguard features, or additional safety mitigation features.

Once the system upgrade has been determined, it is important to evaluate the impacts of the system upgrade on the mission of the facility and the cost. When balance is achieved in the level of risk and upgrade impact on cost, mission, and schedule, the upgraded system is ready for implementation. At this point, the design/analysis process is complete.

17. Grammar. Active Voice.

Grammar tasks

Task A. State grammar tenses. Put questions and write negative sentences.

1. Most people measure the cost of security high.
2. The evaluation helped consumers to determine the level of security of IT product or system.
3. Computer systems security will protect the system against intentional acts.

4. Security officers have to develop an effective policy.

5. Computer security has played an important role in any organization policy for the last 30 years.

6. Business functions become increasingly dependent on small computer systems.

7. Responsibility for the business functions lies with senior executives.

8. A successful security program consists of a number of interrelated key elements.

Choose the correct form of the verb (Present Perfect/Past Simple).

1. We *worked/have worked* over this project since I *came/have come* to the department.

2**.** We *developed/have developed* this program in 2005.

3. At last he *presented/has presented* his report.

4. When *did you finish/have you finished* this work?

5. This laboratory *specialized / has specialized* on the development of electronic protection means and they *just signed / have just signed* a contract.

6. Security police *successfully completed / have successfully completed* the evaluation of the risk.

7. The specialists of Risk Protection *recently published / have recently published* the results of their research.

8. Our engineers *tested / have tested* this device last week *and didn't get / haven't* got satisfactory results.

Task B. Put the verbs in brackets in the correct form.

1. Since the early efforts to conduct quantitative risk assessment, it (gain) its supporters and opponents.

2. The National Bureau of Standards (publish) this document in 1979.

3. The article (deal) with artificial intelligence.

4. Your company (realize) the value of developing enterprise-wide security?

5. First some developers (launch) and (develop) quantitative approaches.

6. Custom applications (require) writing unique security code?

7. Dishonest employees (not want) their acts to be discovered.

6. An honest employee (not make) mistakes in data entry.

8. They already (present) their recommendations of information security.

9. A disgruntled employee is one, who (work) for an organization and (want) to cause harm to it.

10. Enterprises around the world (undergo) transformations.

11. Hi! Where (go)? – I (see) my partners in 20 minutes.

12. What you (do)? – I (be) an engineer, but now I (work) as a manager.

13. The train (leave) at 8.48. Hurry up. – OK. I (come).

14. What you (look) for? – I (try) to find my papers.

Task C. Translate into English using Present Perfect or Past Simple.

1. Привет! Давно тебя не видел. Где ты был?

2. Я был в командировке в Лондоне. - Когда вернулся? - Два дня назад.

3. Мы изучили ваше заявление.

4. Мы провели полный анализ рисков на этом предприятии.

5. Ученые разработали этот шифр в 1993 году.

6. Вы расшифровали этот текст? – Еще нет.

7. Стеганографию использовали в древности.

8. Этот алгоритм был запатентован в США.

9. С 2000 года он используется свободно.

18. Communication

1. Prepare a report and take part in the discussion on the topic “The Aspects of Implementing a Security Policy: Ideas and Obstacles”.

2. Present the variety of modern techniques in risk analysis. Discuss their advantages and disadvantages.

3. Work out the protection profile of a building. Present it to your group.

4. Choose one of the presented protection profiles and analyze its quality. Present the analysis in written.

Unit 3. METHODS OF CRYPTOGRAPHY.

Pronunciation

Make sure you pronounce the following words properly:

authenticate [ɔ: 'θentɪkeɪt]	eavesdropper ['i:vzˌdrɔpə]
authenticity ['ɔ:θenˌtɪsɪtɪ]	guarantee [ˌgærən'ti:]
suite [swi:t]	virtual ['və:tjuəl]
adjustment [ə'dʒʌstmənt]	incompatible [ˌɪnkəm'pætəbl]
recipient [rɪ'sɪpɪənt]	interchangeable [ˌɪntə'tʃeɪndʒəbl]
simplify ['sɪmplɪfaɪ]	guard [gɑ:d]
authority [ɔ: 'θɔrɪtɪ]	sign [saɪn]
binary ['baɪnərɪ]	signature ['sɪgnɪtʃə]

Memorize the terms

1. Read the following terms and their definitions and memorize them:

authenticate information – verify the identity of information

decryption – the reverse process of encryption (see encryption)

eavesdropper – person that doesn't have the authority to read the message, someone who tries to get the contents illegally

encryption – the process of coding a message using a cryptographic algorithm

man-in-the middle-attack – a type of attack when there is an eavesdropper between the sender and the receiver

optional authentication of the client – additional identification and verification of the client

plaintext – unencrypted message, text before sending and encryption

2. Match the following words with their synonyms.

a string (of binary)	encrypted text
be exploitable	set
incompatible standards	realization
secure (an application)	mutually exclusive
implementation	a sequence
suite (of tools)	be used
ciphertext	protect

3. Match the following words with their Russian equivalents.

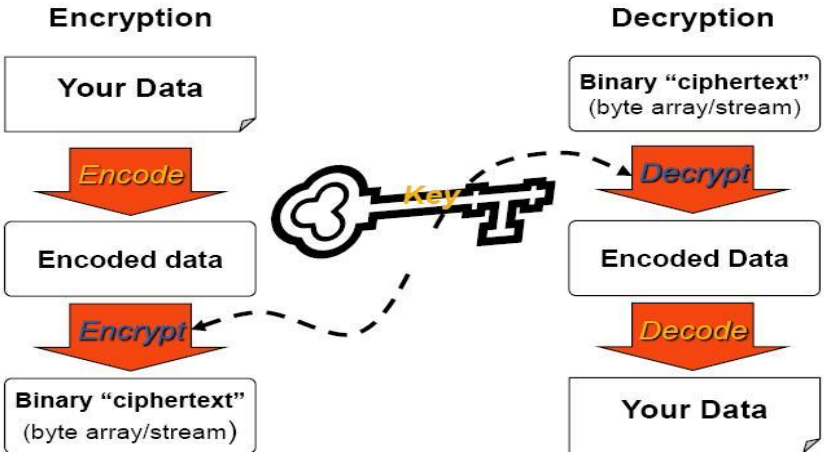
communicating host	атака методом перебора

optional	сервер ключей
standard-conforming protocol	протокол стандартного соответствия
adjustment	дополнительный
brute force (attack)	малофункциональная смарткарта
bulk data	главный компьютер
keyring server	дополнение, приложение
small-ability smartcard	массив данных

Reading

4. Pre-reading task.

What is cryptography? Describe the processes of encryption and decryption basing on the diagram below. What do you know about cryptographic protocols and algorithms?

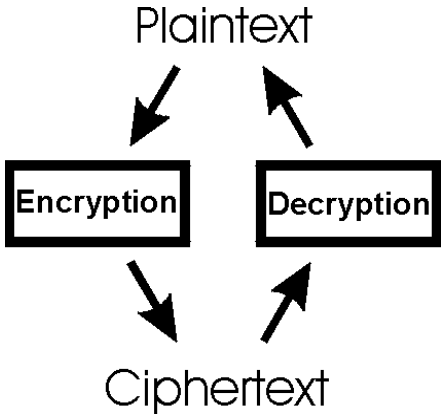


6. Text 1. Read the text and summarize the pieces of advice about cryptographic algorithms.

Cryptographic Algorithms and Protocols.

Cryptography is the science of devising methods that allow information to be sent in a secure form in such a way that the only person able to retrieve this information is the intended recipient.

The basic principle is this: a message being sent is known as **plaintext**. The message is then coded using a cryptographic algorithm. This process is called **encryption.** An encrypted message is known as **ciphertext**, and is turned back into plaintext by the process of **decryption**.



It must be assumed that any eavesdropper has access to all communications between the sender and the recipient. A method of encryption is only secure if even with this complete access, the eavesdropper is still unable to recover the original plaintext from the ciphertext.

In the last few decades cryptographic algorithms, being mathematical by nature, have become sufficiently advanced that they can only be handled by computers. This in effect means that plaintext is binary in form, and can therefore be anything; a picture, a voice, an e-mail or even a video - it makes no difference, a string of binary can represent any of these.

Where possible, use cryptographic techniques to authenticate information and keep the information private (but don't assume that simple

encryption automatically authenticates as well). Generally you'll need to use a suite of available tools to secure your application.

Cryptographic protocols and algorithms are difficult to get right, so do not create your own. Instead, where you can, use protocols and algorithms that are widely-used, heavily analyzed, and accepted as secure. When you must create anything, give the approach wide public review and make sure that professional security analysts examine it for problems. In particular, do not create your own encryption algorithms unless you are an expert in cryptology, know what you're doing, and plan to spend years in professional review of the algorithm.

In general, avoid all patented algorithms - in most cases there's an unpatented approach that is at least as good or better technically, and by doing so you avoid a large number of legal problems.

Often, your software should provide a way to reject ``too small'' keys, and let the user set what ``too small'' is. For RSA keys, 512 bits is too small for use. There is increasing evidence that 1024 bits for RSA keys is not enough either; Bernstein has suggested techniques that simplify brute-forcing RSA, and other work based on it (such as Shamir and Tromer's "Factoring Large Numbers with the TWIRL device") now suggests that 1024 bit keys can be broken in a year by a $10 Million device. You may want to make 2048 bits the minimum for RSA if you really want a secure system, and you should certainly do so if you plan to use those keys after 2015.

When you need a security protocol, try to use standard-conforming protocols such as IPSec, SSL (soon to be TLS), SSH, S/MIME, OpenPGP/GnuPG/PGP, and Kerberos. Each has advantages and

disadvantages; many of them overlap somewhat in functionality, but each tends to be used in different areas:

- Internet Protocol Security (IPSec). IPSec provides encryption and/or authentication at the IP packet level. However, IPSec is often used in a way that only guarantees authenticity of two communicating hosts, not of the users. As a practical matter, IPSec usually requires low-level support from the operating system (which not all implement) and an additional keyring server that must be configured. Since IPSec can be used as a "tunnel" to secure packets belonging to multiple users and multiple hosts, it is especially useful for building a Virtual Private Network (VPN) and connecting a remote machine. As of this time, it is much less often used to secure communication from individual clients to servers. Note that if you use IPSec, don't use the encryption mode without the authentication, because the authentication also acts as integrity protection.
- Secure Socket Layer (SSL) / TLS. SSL/TLS works over TCP and tunnels other protocols using TCP, adding encryption, authentication of the server, and optional authentication of the client (but authenticating clients using SSL/TLS requires that clients have configured X.509 client certificates, something rarely done). SSL version 3 is widely used; TLS is a later adjustment to SSL that strengthens its security and improves its flexibility. SSL/TLS is the primary method for protecting http (web) transactions. A widely used OSS/FS implementation of SSL (as well as other capabilities) is OpenSSL.
- OpenPGP and S/MIME. There are two competing, essentially incompatible standards for securing email: OpenPGP and S/MIME. OpenPHP is based on the PGP application; an OSS/FS implementation is

GNU Privacy Guard from http://www.gnupg.org/. Currently, their certificates are often not interchangeable.

- SSH. SSH is the primary method of securing ``remote terminals'' over an internet, and it also includes methods for tunelling X Windows sessions. However, it's been extended to support single sign-on and general secure tunelling for TCP streams, so it's often used for securing other data streams too (such as CVS accesses). The most popular implementation of SSH is OpenSSH http://www.openssh.com/, which is OSS/FS. Typical uses of SSH allows the client to authenticate that the server is truly the server, and then the user enters a password to authenticate the user (the password is encrypted and sent to the other system for verification). Current versions of SSH can store private keys, allowing users to not enter the password each time. To prevent man-in-the-middle attacks, SSH records keying information about servers it talks to; that means that typical use of SSH is vulnerable to a man-in-the-middle attack during the very first connection, but it can detect problems afterwards. In contrast, SSL generally uses a certificate authority, which eliminates the first connection problem but requires special setup (and payment!) to the certificate authority.
- Kerberos. Kerberos is a protocol for single sign-on and authenticating users against a central authentication and key distribution server. Kerberos works by giving authenticated users "tickets", granting them access to various services on the network. When clients then contact servers, the servers can verify the tickets. Kerberos is a primary method for securing and supporting authentication on a LAN, and for establishing shared secrets (thus, it needs to be used with other algorithms for the actual

protection of communication). Note that to use Kerberos, both the client and server have to include code to use it.

Many of these protocols allow you to select a number of different algorithms, so you'll still need to pick reasonable defaults for algorithms (e.g., for encryption).

6. Answer the following questions.

What are the main terms of cryptography?

What can be a plaintext?

What should a specialist take into account when he wants to create his own or use some developed products?

Which protocols are incompatible?

What is the way to prevent "man-in-the middle" attacks used by SSH?

What key length is considered to be secure to use?

What are the basic characteristics of the cryptographic protocols mentioned in the text?

7. Write if the following statements are true or false.

1. Try to create your own protocol as it'll be more secure.
2. Created protocols should be very carefully tested.
3. A method of encryption is only secure if even with this complete access, the eavesdropper is still unable to recover the original plaintext from the ciphertext.
4. Plaintext is binary so it can be any form.
5. If you use IPSec, you may not use the authentication because the protocol is secure enough to ignore it.
6. Kerberos works by giving authenticated users "tickets", granting them access to various services on the network.

7. If you have the key length equal 1024 you may be sure in the security of your information.
8. Using IPSec is advantageous while building VPNs.

Vocabulary tasks

8. Form different parts of speech.

Verb	**Noun**
encrypt	
	security
authenticate	
	simplicity
Noun	**Adjective**
cryptography	
option	
	communicating

9. Give your definitions of the following terms.

Plaintext, encryption, ciphertext, decryption, optional authentication, vulnerable.

10. Make the word combinations.

1. incompatible	a) of tools
2. communicating	b) protection
3. keyring	c) attack
4. brute	d) authentication
5. integrity	e) standards

6. string	f) information
7. optional	g) force
8. authenticate	h) server
9. man-in-the middle	i) of binary
10. suite	j) host

11. What do the following abbreviations from Text 1 mean?

RSA, IPSec, VPN, SSL.

12. Find abbreviations in Text 2 and comment on their meaning.

13. Complete the text using the words given below.

brute force, encrypt, to break, a key length, hardware

For symmetric-key encryption (e.g., for bulk encryption), don't use ….. less than 90 bits if you want the information to stay secret through 2016 (add another bit for every additional 18 months of security). For encrypting worthless data, the old DES algorithm has some value, but with modern …. it's too easy to break DES's 56-bit key using …. . If you're using DES, don't just use the ASCII text key as the key - parity is in the least (not most) significant bit, so most DES algorithms will …. using a key value well-known to adversaries; instead, create a hash of the key and set the parity bits correctly (and pay attention to error reports from your encryption routine). So-called ``exportable'' encryption algorithms only have effective key lengths of 40 bits, and are essentially worthless; in 1996 an attacker could spend $10,000 …. such keys in twelve minutes or use idle computer time to break them in a few days, with the time-to-break halving every 18 months in either case.

14. Translate into Russian the following paragraph.

Serpent is an AES submission by Ross Anderson, Eli Biham, and Lars Knudsen. Its authors combined the design principles of DES with the recent development of bitslicing techniques to create a very secure and very fast algorithm. While bitslicing is generally used to encrypt multiple blocks in parallel, the designers of Serpent have embraced the technique of bitslicing and incorporated it into the design of the algorithm itself. Serpent uses 128 bit blocks and 256 bit keys. Like DES, Serpent includes an initial and final permutation of no cryptographic significance; these permutations are used to optimize the data before encryption. Serpent was released at the 5th International Workshop on Fast Software Encryption. Serpent 1 resists both linear and differential attacks.

15. Complete the text by translating Russian phrases given in brackets.

The use of public key cryptography is thus conceptually simple. But two immediate worries may spring to mind. A first concern is that although (1 взломщик, перехватив закодированное послание Эллис) will only see gibberish, the intruder knows both the key (Bob's public key, (2 который доступен всем) and the algorithm that Alice used for encryption. Trudy can thus mount (3 выбранную атаку текста), using the known standardized encryption algorithm and Bob's publicly available encryption key to encode any message she chooses. Trudy might well try to encode messages, or parts of messages she chooses. Trudy might well try, for example, to encode messages, or parts of messages, that she suspects that Alice might send. Clearly, if public key cryptography is to work, (4 подбор ключа) and encryption/decryption must be done in such a

way that it is impossible (or at least so hard to be impossible for all practical purposes) for an intruder to either determine Bob's private key or somehow otherwise (5 расшифровать или угадать) Alice's message to Bob. A second concern is that since Bob's encryption key is public, (6 любой может отправить зашифрованное послание Бобу), including Alice or someone claiming to be Alice. In the case of a single shared secret key, the fact that the sender knows the secret key (7 косвенно устанавливает отправителя). In the case of public key cryptography, however, this is no longer the case since anyone can send an encrypted message to Bob using Bob's publicly available key. Certificates, which we will study later, (8 необходимы для того, чтобы соотнести человека и конкретный открытый ключ).

16. Translate into English

Хотя существует много алгоритмов и ключей, обладающих этим свойством, алгоритм РСА (названный в честь его разработчиков Р. Райвеста, А.Шамира и Л.Эйдмана) стал практически синонимом криптографических систем с открытым ключом. Рассмотрим сначала, как работает алгоритм РСА. Предположим, Боб хочет отправить зашифрованное сообщение. РСА состоит из двух взаимосвязанных компонентов:

– выбора открытого и закрытого ключа,

– алгоритма зашифрования и расшифрования.

17. Translate into English

DES алгоритм является первым примером широкого производства и внедрения технических средств в область защиты информации. К настоящему времени выпускается несколько десятков

устройств аппаратно - программной реализации DES-алгоритма. Для выпуска такого рода устройства необходимо получить сертификат Национального Бюро Стандартов на право реализации продукта, который выдается только после всесторонней проверки.

Достигнута высокая скорость шифрования. По некоторым сообщениям, в одном из устройств на основе специализированной микросхемы она составляет около 45 Мбит/сек.

Основные области применения DES-алгоритма:

- хранение данных в ЭВМ (шифрование файлов, паролей);

- электронная система платежей (между клиентом и банком);

- электронный обмен коммерческой информацией (между покупателем и продавцом).

18. Read the text and underline the sentences with the information about the basic algorithms and the sphere of their application.

Text 2. Symmetric Key Encryption Algorithms. Public Key Algorithms. Cryptographic Hash Algorithms.

The use, export, and/or import of implementations of encryption algorithms are restricted in many countries, and the laws can change quite rapidly. Find out what the rules are before trying to build applications using cryptography.

For secret key (bulk data) encryption algorithms, use only encryption algorithms that have been openly published and withstood years of attack, and check on their patent status. We would recommend using the new Advanced Encryption Standard (AES), also known as Rijndahl -- a number of cryptographers have analyzed it and not found any serious weakness in it, and we believe it has been through enough analysis

to be trustworthy now. However, in August 2002 researchers Fuller and Millar discovered a mathematical property of the cipher that, while not an attack, might be exploitable into an attack. A good alternative to AES is the Serpent algorithm, which is slightly slower but is very resistant to attack. For many applications triple-DES is a very good encryption algorithm; it has a reasonably lengthy key (112 bits), no patent issues, and a very long history of withstanding attacks. Twofish appears to be a good encryption algorithm, but there are some lingering questions - Sean Murphy and Fauzan Mirza showed that Twofish has properties that cause many academics to be concerned. MARS is highly resistent to ``new and novel'' attacks, but it's more complex and is impractical on small-ability smartcards. Your protocol should support multiple encryption algorithms, anyway; that way, when an encryption algorithm is broken, users can switch to another one.

For symmetric-key encryption (e.g., for bulk encryption), don't use a key length less than 90 bits if you want the information to stay secret through 2016 (add another bit for every additional 18 months of security). For encrypting worthless data, the old DES algorithm has some value, but with modern hardware it's too easy to break DES's 56-bit key using brute force. If you're using DES, don't just use the ASCII text key as the key - parity is in the least (not most) significant bit, so most DES algorithms will encrypt using a key value well-known to adversaries; instead, create a hash of the key and set the parity bits correctly.

Block encryption algorithms can be used in a number of different modes, such as ``electronic code book'' (ECB) and ``cipher block chaining'' (CBC). In nearly all cases, use CBC, and do *not* use ECB mode -

in ECB mode, the same block of data always returns the same result inside a stream, and this is often enough to reveal what's encrypted. Many modes, including CBC mode, require an ``initialization vector'' (IV). The IV doesn't need to be secret, but it does need to be unpredictable by an attacker.

There are a number of different streaming encryption algorithms, but many of them have patent restrictions. If you use RC4, use it as intended - in particular, always discard the first 256 bytes it generates, or you'll be vulnerable to attack. SEAL is patented by IBM - so don't use it. SOBER is patented.

For public key cryptography there are only a few widely-deployed algorithms. One of the most widely-used algorithms is RSA. The Diffie-Hellman key exchange algorithm is widely used to permit two parties to agree on a session key.

NIST developed the digital signature standard (DSS) for digital signature generation and verification; one of the conditions for its development was for it to be patent-free.

RSA, Diffie-Hellman, and El Gamal's techniques require more bits for the keys for equivalent security compared to typical symmetric keys. A 512-bit RSA key is considered completely unsafe. In the past, a 1024-bit RSA key was considered reasonably secure, but recent advancements in factorization algorithms (e.g., by D. J. Bernstein) have raised concerns that perhaps even 1024 bits is not enough for an RSA key.

If you need a public key that requires far fewer bits (e.g., for a smartcard), then you might use elliptic curve cryptography (IEEE P1363 has some suggested curves; finding curves is hard).

Some programs need a one-way cryptographic hash algorithm, that is, a function that takes an ``arbitrary'' amount of data and generates a fixed-length number that hard for an attacker to invert. For a number of years MD5 has been a favorite, but recent efforts have shown that its 128-bit length may not be enough and that certain attacks weaken MD5's protection.

19. Grammar. Passive Voice. See Grammar reference.

Task A. Choose the correct form of Passive Voice.

1. The assumed threats to security *specify/ specified/are specified* below.
2. The unauthorized disclosure *has been prevented/has prevented/has being prevented.*
4. The repeatable key *based/is based/bases* on the following principles.
5. Knowing about the risk, one *is prepares/prepared/is prepared* better to protect information.
6. A sound IRM program *founds/founded/is founded* on a well thought out IRM policy infrastructure.
7. An event, the occurrence of which could have an undesirable impact, *is defined/define/ defines* as threat.
8. Nowadays real-time operating system *is employed/are employed/were employed* in consumer devices.
9. The underlined secure network services *installed/was installed/were installed* in accordance with the operational documentation.

Task B. Put the verbs in brackets in the correct form of Passive Voice.

1. Uncertainty (measure) inversely with the respect to confidence.
2. The papers of the conference (translate) into 12 languages.

3. Both expected frequency and exposure factor for fire (increase) by not having a fire suppression system.
4. Exposure factor (express) as a percent.
5. Generally accepted Information Security Principles (base) on an Authoritative Foundation of supporting documents and guidelines.
6. It is essential that the process of analyzing and assessing risk (understand) by all sides.
7. It (discover) that 1024 bits is not enough for an RSA key.
8. The program (develop) for about three months before some mistakes (find) in it.
9. New tools for solving this problem (design) now.
10. By the end of the term the students (master) new technicues.

Task C. Put the verbs in brackets in the correct form, Active or Passive Voice.

1. The curves (show) in figure 4.
2. Our analysis (suggest) the spheres of practical application of our technique.
3. Our ongoing work (focus) on the use of other biometric measurements.
4. If the BUSINESS module (choose) this can (use) to generate a detailed questionnaire appropriate to the system under review.
5. W.F.Friedman's monograph «The Index of Coincidence and its Application in Cryptography» (appear) in 1918.
6. These systems (share) an unmatched reputation for operating 24 hours a day, 365 a year, nonstop.

7. Back in the 90-s, Anti-virus researchers first (fight back) by creating special detection routines designed to catch each polymorphic virus, one by one.

8. By hand, line by line, they (write) special programs.

9. US Army and Navy (work) entirely in secret, when their specialists (begin) making fundamental advances in cryptography.

10. H.Feistel, who earlier (work) on identification friend or foe devices for the Air Force, (change) the sphere of his scientific interests.

20. Communication.

Prepare a report and take part in the discussion on the topic "New and Novel Cryptographic Algorithms".

Questions for discussion.

Which ideas made the greatest contribution to the development of cryptography (present them in chronological order)?

What are the most famous cryptographic algorithms?

What do you know about their developers?

Which facts from the history of cryptography impressed you most of all?

Unit 4. MODERN METHODS OF CRYPTANALYSIS.

Pronunciation

Make sure you pronounce the following words properly:

incomprehensible [ɪŋkɔmprɪˈhensəbl]	drudgery ['drʌdʒərɪ]

cipher ['saɪfə]	avalanche ['ævəlɑ:nʃ]
altitude ['æltɪtju:d]	precede [prɪ'si:d]
finite ['faɪnaɪt]	genetic [dʒɪ'netɪk]
mimic ['mɪmɪk]	quantitative ['kwɔntɪtətɪv]
endure [ɪn'djuə]	mutate [mju:'teɪt]
subtle ['sʌtl]	duplicate ['djuɪplɪkət]
trial ['traɪəl]	inheritance [ɪn'herɪtəns]

Memorize the terms

1. Read the following terms and their definitions and memorize them:

avalanche property of DES - changing a single bit in a DES key results in every bit of the enciphered block being changed randomly after only a few rounds

ciphertext-only solution – process of decryption when cryptanalyst has only encrypted text to recover the plaintext

endure – bear, stand, suffer, sustain

flaw – disadvantage, demerit, weak point in the system

incomprehensible ciphertext – encrypted message that is impossible to read and understand

mimic the process – imitate, simulate the process

overlapping superencipherment groups – partial matching of encrypted messages

remove one bit of drudgery – simplify monotonous work

subtle – delicate, gentle, hardly seen

2. Match the following words with their Russian equivalents.

chain of discrete elements	отсеченный дифференциал
avalanche property of DES	исключающее «или»
hill climbing algorithm	конечный автомат
truncated differential	алгоритм нахождения экстремума
finite state machine	пробный ключ
xor	лавинное свойство DES
encipher the known plaintext	последовательность дискретных компонентов
trial key	зашифровать имеющийся (известный) открытый текст

3. Match the following words with their synonyms.

unrelated (characteristics)	scaling, computation, evaluation
overlapping	punched card machines
consistent	unreadable, impossible to understand
obtain clue	not connected
converted unit record equipment	derive, extract, obtain key
incomprehensible	match, coincide
calculus	compatible

Reading

4. Pre-reading task.

What do you know about cryptanalysis? What cryptographic algorithms can you name?

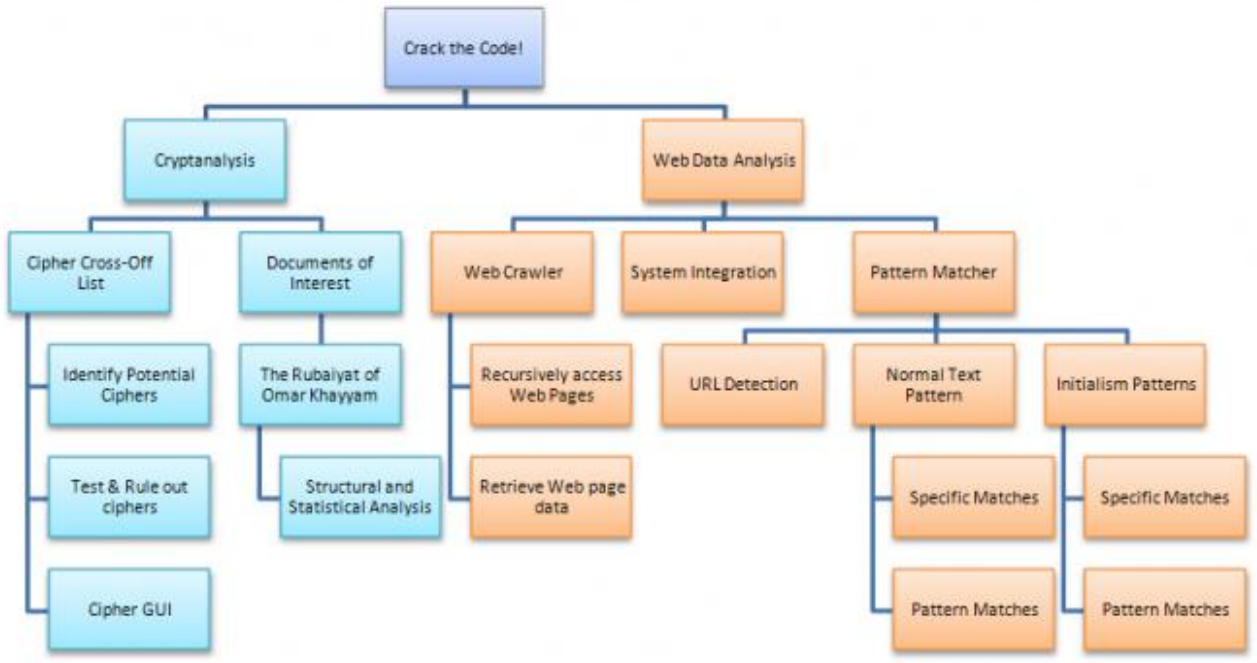
5. Read the text and find out if it mentions the following:

1. Cryptanalysis requires hard work and intelligence.
2. Automated aids are of great help with modern cipher systems.
3. In AI approach it is tried to combine the speed of the computer with the way a human cryptanalyst works.
4. Hill climbing algorithm provides solutions of DES algorithm.
5. Genetic programming is a method by which a computer produces an answer to a question by mimicing the process of natural selection.

Text 1. Cryptanalysis.

Cryptanalysis is hard work, requiring a willingness to endure many false starts, and a painstaking attention to detail. It requires intelligence to see subtle patterns in incomprehensible ciphertext.

Automated aids to cryptanalysis come in many forms. Some collected statistical information about ciphertexts, thus removing one bit of drudgery from human shoulders. Others, such as the Bombe used in attacking the German Enigma, or the DES cracker built by the Electronic



Frontier Foundation, or the converted unit record equipment (punched card machines) which compared Japanese code messages to one another at various displacements to find messages with overlapping superencipherment groups, work by trying thousands, or millions, of possibilities, one after another.

Neither of these techniques is adequate to deal with many cipher systems, particularly modern ones. A well-designed cipher will not offer a simple opportunity to try different possibilities to find partial information about the key, and will have a key large enough to make trying every possible key hopeless. Nor is ordinary statistical information about the frequencies and contacts of bytes in the ciphertext likely to be much use.

Thus, approaches taken from the field of AI (*artificial intelligence*) have been tried. In these approaches, it is attempted to combine the speed of the computer with steps that at least slightly move towards the skill and judgement of a human cryptanalyst.

Hill-climbing

Because the individual bits of the subkeys in DES are actual bits taken from the 56-bit DES key, an approach like the following to recover a DES key must have occurred to many people.

Given a block of known plaintext, and its corresponding ciphertext, starting with a random 56-bit possible key, do the following:

- Encipher the known plaintext with that key, and with every one of the 56 other keys obtained by inverting one bit of that key.
- Compare the resulting ciphertext to the actual ciphertext.
- In those of the 56 cases where the flipped bit results in the ciphertext produced differing in fewer bits from the actual ciphertext than that

produced by the original trial key, invert that bit of the trial key to obtain the next trial key.

This is a simple example of a hill-climbing algorithm, where the number of bits by which a trial encipherment differs from the actual ciphertext is a measure of one's (lack of) altitude.

It would, however, never work against DES. That is because of the *avalanche property* of DES; changing a single bit in a DES key results in every bit of the block being enciphered being changed randomly after only a few rounds.

Thus, even attempting to improve the hill climbing algorithm above by, for each trial, enciphering the known plaintext for eight rounds with the trial key, and deciphering the actual ciphertext for eight rounds with the trial key, and then determining the number of bits by which these two results differed would not be enough to help.

Another idea would be to choose two rounds of DES, and by determining the input to those rounds by enciphering the known plaintext by the previous rounds, and the required output from those rounds by deciphering the actual ciphertext by the following rounds, examine the two 48-bit subkeys for the rounds, and, by examining the four possibilities for each group of 6 bits in those subkeys to produce the required change in each half of the block, find those which are consistent with the origin of those two subkeys from the original 56-bit key, and then try the resulting new 56-bit key or keys on the basis that it or they might be improvements over the preceding trial key.

Genetic Programming

A thesis by A. J. Bagnall described the ciphertext-only solution of some simple rotor machines by means of the technique of genetic programming.

Genetic programming is a method by which a computer produces an answer to a question, or even a computer program to perform a task, by mimicing the process of natural selection. As noted in the thesis, and in the book *Artificial Life* by Stephen Levy, this technique was originated by John Holland in the mid-1960s, and his student David Goldberg was one of the first to refine the technique so that it could be used in practice with real problems of importance.

It can be thought of as a special case of the hill-climbing algorithm, in that a quantitative measure of how "warm" the computer is in approaching the desired solution is required.

Programs or answers must be in the form of a chain of discrete elements, such that there is at least a reasonable likelihood that a chain formed by taking one chain, and replacing a span of elements within it by the corresponding elements from another chain, will "make sense". Random mutations are also usually used, although genetic crossover has been found to be much more important.

Starting with a random selection of solutions, those that work best are retained, and used as the parents of the next generation of solutions to be tried. Often, this retention is also randomized, so that better solutions have a higher probability of being retained.

One type of mutation that happens in real life has not, to my knowledge, been used for genetic programming yet. Occasionally, plants and animals will increase the size of their genetic inheritance by

duplicating part of it. Thus, a finite state machine could mutate by becoming a machine with twice as many states. It might be useful to make provision for this where a problem might be more complex to solve than initially realized.

6. Answer the following questions.

What automated aids to cryptanalysis do you remember? Characterize them in a few words.

What are the approaches to cryptanalysis?

What are the specific feature and potential of AI approach?

What fact is the idea of hill-climbing algorithm based on?

What does avalanche property of DES mean?

What are the tendencies in genetic programming?

Vocabulary tasks

7. Form different parts of speech and translate them.

Verb	**Noun**
	mutation
approach	
comprehend	
inherit	
	origin

8. Give as many word combinations as possible and translate them.

Key, solution, cipher.

9. Make the word combinations.

1. ciphertext-only	a) a DES key

2. flipped	b) ciphertext
3. hill climbing	c) aids
4. trial	d) the process
5. recover	e) bit results
6. mimic	f) of discrete elements
7. incomprehensible	g) solution
8. chain	h) algorithm
9. automated	i) group
10. superencipherment	j) key

10. Complete the text using the terms and word combinations given below.

Running through, a strong encryption algorithm, maps, in parallel, the cryptanalyst, the actual message, computing power

There are several distinct types of cryptoanalytic attack. The type used depends on the type of cipher and how much information ….. has.

Types of cryptoanalytic attacks. A standard cryptoanalytic is to determine the key which … a known plaintext to a known ciphertext. This plaintext can be known because it is standard or because it is guessed. If the plaintext segment is guessed it is unlikelely that its exact position is known however a message is generally short enough for a cryptoanalyst to try all possible positions … . In some systems a known ciphertext-plaintext pair will compromise the entire system however … will be unbreakable under this type of attack.

A brute force attack requires a large amount of … and a large amount of time to run. It consists of trying all possibilities in a logical manner until the correct one is found. Another type of brute force attack is a dictionary attack. This essentially involves … a dictionary of words in the hope that the key (or the plaintext) is one of them. This type of attack is often used to determine passwords since people usually use easy to remember words.

In a ciphertext only attack the cryptanalyst has only the encoded message from which to determine the plaintext, with no knowledge whatsoever of ….

11. Complete the text.

Given a block of known plaintext, and its corresponding … , starting with a random 56-bit possible key, do the following:

- … the known plaintext with that key, and with every one of the 56 other keys obtained by inverting one bit of that key.
- Compare the resulting ciphertext to the … ciphertext.
- In those of the 56 cases where the flipped bit results in the ciphertext produced … in fewer bits from the actual ciphertext than that produced by the original trial key, invert that bit of the trial key to obtain the next trial key.

This is a simple example of a … algorithm, where the number of bits by which a trial encipherment differs from the actual ciphertext is a measure of one's (lack of) altitude.

12. Translate into English the following passage.

Осуществляя атаку, криптоаналитик может ставить целью решение следующих задач: получение открытого текста из зашифрованного, вычисление ключа шифрования.

Вторая из перечисленных задач является существенно более сложной, чем первая. Однако, имея ключ шифрования, криптоаналитик может впоследствии расшифровывать все данные, зашифрованные найденным ключом. Такая атака (в случае ее успешного осуществления) называется *полным раскрытием* алгоритма шифрования.

Атаки на алгоритмы шифрования принято классифицировать в зависимости от того набора информации, который имеет злоумышленник перед осуществлением своей атаки.

13. Read the text, choose one type of ciphers and characterize it orally.

Text 2.

Cryptanalytic Methods for Modern Ciphers.

Block ciphers like DES are intended to be very hard to break, and they are largely successful in achieving this. Having even copious quantities of corresponding plaintext and ciphertext, it is intended that the fastest way to discover the key, so as to be able to decrypt other messages, would be a *brute-force search*, that is, trying every possible key until the right one is found.

Many block ciphers appear to meet this condition. Two cryptanalytic methods that can do slightly better with some of the earlier block ciphers, such as DES and LUCIFER, are *differential cryptanalysis* and *linear cryptanalysis*.

Differential Cryptanalysis. However, if one is fortunate enough to have a large quantity of corresponding plaintext and ciphertext blocks for a particular unknown key, a technique called differential cryptanalysis, developed by Eli Biham and Adi Shamir, is available to obtain clues about some bits of the key, thereby shortening an exhaustive search.

After two rounds of DES, knowing both the input and output, it is trivial to determine the two subkeys used, since the outputs of both f-functions are known. For each S-box, there are four possible inputs to produce the known output. Since each subkey is 48 bits long, but the key is only 56 bits long, finding which of the four possibilities is true for each group of six bits in the subkeys is a bit like solving a crossword puzzle.

As the number of rounds increases, though, the simple correlations disappear. Differential cryptanalysis represents an approach to finding more subtle correlations.

In fact, however, a complete pattern of which bits change and do not change in the input and in the output is the subject of differential cryptanalysis. The basic principle of differential cryptanalysis, in its classic form, is this: the cipher being attacked has a *characteristic* if there exists a constant X such that given many pairs of plaintexts A, B, such that B = A xor X, if a certain statement is true about the key, E(B,k) = E(A,k) xor Y for some constant Y will be true with a probability somewhat above that given by random chance.

Linear Cryptanalysis. Linear cryptanalysis, invented by Mitsuru Matsui, is a different, but related technique. Instead of looking for isolated points at which a block cipher behaves like something simpler, it involves trying to create a simpler approximation to the block cipher as a whole.

For a great many plaintext-ciphertext pairs, the key that would produce that pair from the simplified cipher is found, and key bits which tend to be favored are likely to have the value of the corresponding bit of the key for the real cipher. The principle is a bit like the summation of many one-dimensional scans to produce a two-dimensional slice through an object in computer-assisted tomography.

Truncated differentials. It is of course possible that some of the bits of E(A,k) xor E(B,k) will be more likely to match those of Y than others. If one can, in addition, ignore some of the bits of A and B, one has a *truncated differential* for the cipher being attacked, and this technique, due to Lars R. Knudsen, has been found to be very powerful.

Higher-order Differentials. Another important addition to the available techniques deriving from differential cryptanalysis is the use of higher-order differentials, which first appeared in a paper by Xuejia Lai.

A differential characteristic of the type described above, where for a large number of different values of A, B equals A xor X, and the encrypted versions of A and B for a given key, k, are expected to have the relation E(A,k) = E(B,k) xor Y, if a target statement about the key k is true, can be made analogous to a derivative in calculus, and then it is termed that Y is the first derivative of the cipher E at the point X.

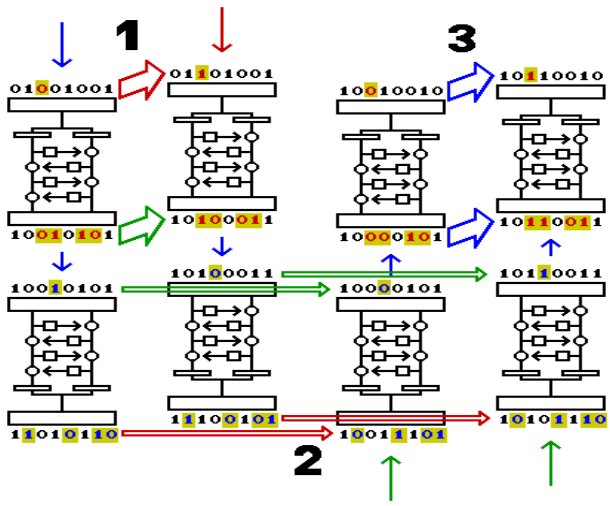
A second-order derivative would then be one involving a second quantity, W, such that E(A,k) xor E(B,k) = E(C,k) xor E(D,k) xor Z is expected to be true more often than would be true due to chance, where not only is B = A xor X, but C = A xor W and D = B xor W. In that case, Z is the second derivative of the cipher E at the point X,W. Since xor performs the function of addition and subtraction, the four items encrypted

for any A are just lumped together in this case, but if differential cryptanalysis were being performed over another field where the distinction is significant, then Y=E(A+X,k)-E(A,k) and Z=(E(A+X+W,k)-E(A+W,k))-(E(A+X,k)-E(A,k)) would be the appropriate equations to use.

The Boomerang Attack. Recently, a means of improving the flexibility of differential cryptanalysis was discovered by David A. Wagner. Called the *boomerang attack*, it allows the use of two unrelated characteristics for attacking two halves of a block cipher.

This diagram shows how the attack might work if everything goes perfectly for a particular initial block.

1. Start with a random block of plaintext. Based on the characteristic known for the first half of the cipher, if we XOR a certain vector with it, called **d1** (equal to 00100000 in the diagram), the result after half-enciphering the two plaintext blocks, before and after the XOR, will differ by **c1** (equal to 00110110 in the diagram), *if* what we wish to learn about the key happens to be true.



2. Since the characteristic applies only to the first half of the cipher, the results after the whole block cipher won't be related. Take those two results and XOR each one with **d2** (equal to 01001011 in the diagram), which is the vector corresponding to the characteristic for the second half of the cipher. In each case, XORing **d2** with a ciphertext block is expected to change the result after

deciphering halfway by **c2** (equal to 00010000 in the diagram), again, *if* something is true of the key.

3. With two intermediate results that differ by **c1**, if each one has **c2** XORed to it, the two results of the XOR will still differ by **c1**. Since this difference now relates to the *first* half characteristic, it can be seen in the final output, thus indicating the truth or otherwise of two hypotheses about the key.

This increases the potential effectiveness of differential cryptanalysis, because one can make use of characteristics that do not propagate through the complete cipher.

14. Grammar. Active and Passive Voice. See Grammar Reference.

Grammar tasks.

Task A. Choose the correct form.

1. We're sure this approach *will/is going to* be unique.
2. We *will/are going to* buy new equipment.
3. This laboratory *will/is going to* work over a speech synthesizer.
4. I've got problems with this program. – I *will/am going to* help you.
5. In this case unauthorized physical access *will prevent/will be prevented/will prevented*.
6. Knowing about the risk, one *is prepares/will prepared/will be prepared* to mitigate it.
7. The underlined secure network services *will be installed/will have been installed/is installed* in accordance with the operational documentation.

8. A two-dimensional slice through an object *will produce/will be produced/will produced* by the summation of many one-dimensional scans in computer-assisted tomography.

9. The project *will launch/will be launched/will have been launched* by the end of the month.

10. Big credit card companies *will develop/will be developed/are going to develop* more secure ways to use credit cards.

Task B.

Put the verbs in brackets in the correct form of Passive Voice.

1. This work (finish) next month.
2. The papers of the conference (translate) into 12 languages.
3. The system (develop) by 2010.
4. It is essential that the process of analyzing and assessing risk (understand) by all sides.
5. By the end of the year all the problems (settle).
6. You (inform) about the decision of the consumers in a week.

Complete the sentences with the verbs in brackets and *will/going to.*

1. Could you meet our colleagues at the airport? – OK. I (do) it.
2. I (launch) this program tomorrow.
3. Where you (stay) in London?
4. I think biometrics (use) for identification and authentication everywhere.
5. I (present) our research at the conference in Moscow in June
6. At this time next year we (discuss) the details of the experiment.
7. Our scientists (develop) modern equipment next month. All arrangements have been made.

8. We hope that the new device (develop) next year.

Task C. Put the verbs in brackets into a suitable form.

1. Don’t phone between 8.00 and 14.00. We (make) a presentation.
2. By the time he (arrive) at the office the work already (start).
3. According to the timetable the bus (arrive) at 8. Chris (come) an hour later.
4. We (meet) at the airport tomorrow.
5. If the BUSINESS module (choose) this (use) to generate a detailed questionnaire appropriate to the system under review.
6. Our consumers (hope) the results of the risk assessment (obtain) soon.
7. C.E. Shannon (develop) a method for symbolic analysis of switching systems and networks in the late 1930-s.
8. He (work) at Bell laboratories when he (publish) a paper on information theory.
9. He and his IBM colleagues (contribute) to the early research in this field.
10. Rochester (take part) in the MIT artificial Intelligence Project.
11. When we (come), the professor (deliver) the lecture.

15. Communication.

Prepare a report about the development of first automation tools for cryptanalysis.

Dwell on the history of cryptanalysis in Russia.

Prepare a report and take part in the discussion on the topic: Modern Trends in Cryptanalysis.

Make a table containing the analysis of modern cryptanalytic methods. Present the table to the group and discuss it.

Unit 5. STEGANOGRAPHY.

Pronunciation

Make sure you pronounce the following words properly:

covert ['kʌvət]	subtle ['sʌtl]
nefarious [nɪ'fɛərɪəs]	flourish ['flʌrɪʃ]
fraud [frɔ:d]	innocent ['ɪnəsənt]
unreadable [ˌʌn'ri:dəbl]	medium ['mi:djəm]
analogy [ə'nælədʒɪ]	template ['templɪt]
categorize ['kætɪgəraɪz]	carrier ['kærɪə]
espionage [ˌespɪə'nɑ:ʒ]	technique [tek'ni:k]

Memorize the terms

1. Read the following terms and their definitions and memorize them:

carrier text **-** – place where secret message is kept

coin a term – invent and introduce

doodle – flourish, additional dash in the letter

grille cipher – cipher that can be decrypted using special grid put on the message hidden in the carrier text

retrieve the hidden text – restore, reconstruct the secret message

semagram – secret message where any symbols can be used except letters and figures

steganography medium – concept that includes hidden_message, carrier and steganography_key

2. Match the following words with their Russian equivalents.

digital watermarking	поразрядно идентичный
doodle	трафаретный шифр
cue code	сжатие с потерей данных
bit-for-bit identical	нулевой код
treat	ключевой код
null cipher	рассматривать
grille cipher	дополнительный штрих в букве
lossy compression	нанесение (цифровых) водяных знаков (меток)

3. Match the following words with their synonyms.

covert communication	side
nefarious application	simulation, imitation
intend	built in
microdot	secret, stealthy interaction
(spam) mimic	deception, cheating
party	tiny photograph

embed	be about, be going to
(financial) fraud	dishonest, corrupt using

Reading

4. Pre-reading task.

Look at the title of the text. What information do you expect to read here?

What would you like to know about steganography?

Where have you met steganographic techniques?

5. Text 1. Read the text and give brief characteristics of the main steganographic techniques.

Steganography.

Steganography is the art of covered or hidden writing. The purpose of steganography is covert communication to hide a message from a third party. This differs from cryptography, the art of secret writing, which is intended to make a message unreadable by a third party but does not hide the existence of the secret communication. Although steganography is separate and distinct from cryptography, there are many analogies between the two, and some authors categorize steganography as a form of cryptography since hidden communication is a form of secret writing. Nevertheless, this paper will treat steganography as a separate field.

Although the term steganography was only coined at the end of the 15th century, the use of steganography dates back several millennia. In ancient times, messages were hidden on the back of wax writing tables, written on the stomachs of rabbits, or tattooed on the scalp of slaves. Invisible ink has been in use for centuries—for fun by children and students and for serious espionage by spies and terrorists. Microdots and

microfilm, a staple of war and spy movies, came about after the invention of photography.

Steganography hides the covert message but not the fact that two parties are communicating with each other. The steganography process generally involves placing a hidden message in some transport medium, called the carrier. The secret message is embedded in the carrier to form the steganography medium. The use of a steganography key may be employed for encryption of the hidden message and/or for randomization in the steganography scheme. In summary:

steganography_medium = hidden_message + carrier + steganography_key

Figure 1 shows a common taxonomy of steganographic techniques.

- Technical steganography uses scientific methods to hide a message, such as the use of invisible ink or microdots and other size-reduction methods.

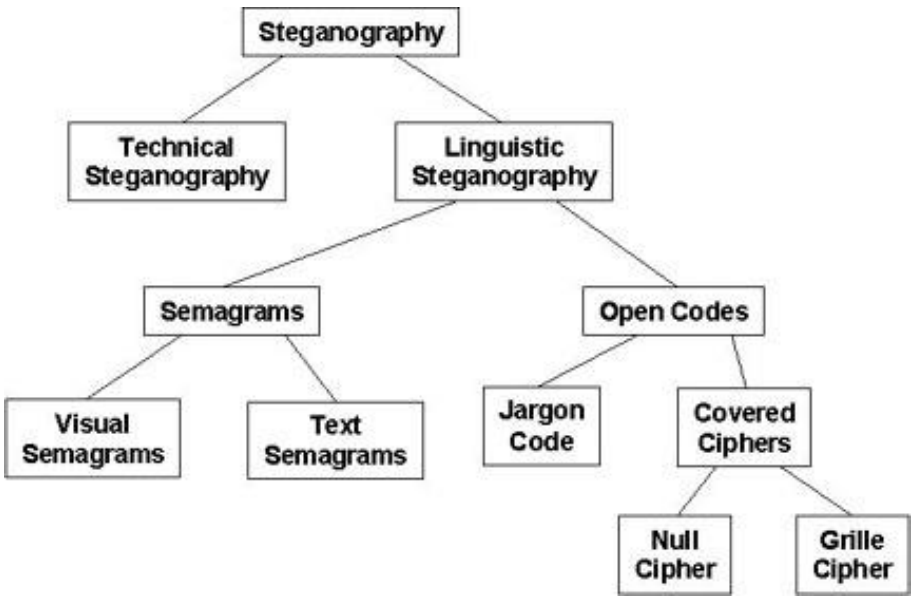


Figure 1. Classification of Steganography Techniques (Adapted from Bauer 2002)

- Linguistic steganography hides the message in the carrier in some nonobvious ways and is further categorized as semagrams or open codes.
- Semagrams hide information by the use of symbols or signs. A visual semagram uses innocent-looking or everyday physical objects to convey a message, such as doodles or the positioning of items on a desk or Website. A text semagram hides a message by modifying the appearance of the carrier text, such as subtle changes in font size or type, adding extra spaces, or different flourishes in letters or handwritten text.
- Open codes hide a message in a legitimate carrier message in ways that are not obvious to an unsuspecting observer. The carrier message is sometimes called the overt communication, whereas the hidden message is the covert communication. This category is subdivided into jargon codes and covered ciphers.
- Jargon code, as the name suggests, uses language that is understood by a group of people but is meaningless to others. Jargon codes include warchalking (symbols used to indicate the presence and type of wireless network signal, underground terminology, or an innocent conversation that conveys special meaning because of facts known only to the speakers). A subset of jargon codes is cue codes, where certain prearranged phrases convey meaning.
- Covered or concealment ciphers hide a message openly in the carrier medium so that it can be recovered by anyone who knows the secret for how it was concealed. A grille cipher employs a template that is used to cover the carrier message. The words that appear in the openings of the template are the hidden message. A null cipher hides the message

according to some prearranged set of rules, such as "read every fifth word" or "look at the third character in every word."

As an increasing amount of data is stored on computers and transmitted over networks, it is not surprising that steganography has entered the digital age. On computers and networks, steganography applications allow for someone to hide any type of binary file in any other binary file, although image and audio files are today's most common carriers.

Steganography provides some very useful and commercially important functions in the digital world, most notably digital watermarking. In this application, an author can embed a hidden message in a file so that ownership of intellectual property can later be asserted and/or to ensure the integrity of the content. An artist, for example, could post original artwork on a Website. If someone else steals the file and claims the work as his or her own, the artist can later prove ownership because only he/she can recover the watermark. Although conceptually similar to steganography, digital watermarking usually has different technical goals. Generally only a small amount of repetitive information is inserted into the carrier, it is not necessary to hide the watermarking information, and it is useful for the watermark to be able to be removed while maintaining the integrity of the carrier.

Steganography has a number of nefarious applications; most notably hiding records of illegal activity, financial fraud, industrial espionage, and communication among members of criminal or terrorist organizations.

6. Answer the following questions.

What is the purpose of steganography?

How is steganography related to cryptography?

What was the early use of steganography?

What is carrier?

How can you define steganography medium?

What is the application of steganography nowadays?

7. Mark the following statements "true" or "false". Correct the false statements.

1. Steganography is the art of hiding the existence of secret communication.
2. Steganography got its name several millennia back.
3. Steganography is related to cryptography.
4. Carrier is a special medium where the secret message is put.
5. Jargon codes use special phrases with the meaning that is not understood by malicious users.
6. Technical steganography changes the way the carrier text looks by adding extra spaces or using different flourishes.
7. Digital watermarking is one of the modern steganography techniques.
8. Cue codes are a subclass of grille ciphers.
9. A visual semagram modifies the appearance of the carrier text.
10. Null cipher is a kind of linguistic steganography.

Vocabulary tasks

8. Remember word combinations containing the following terms and translate them.

Steganography, cipher, code, medium, message, communication.

9. Make the word combinations

1. digital	a) communication
2. size-reduction	b) code
3. covert	c) application
4. open	d) fraud
5. nefarious	e) text
6. nonobvious	f) watermarking
7. cue	g) a message
8. convey	h) method
9. carrier	i) code
10. financial	j) way

10. Complete the text using the terms and word combinations given below.

Apparent message, covered, illegal, a transport layer, the visible lines, suspicion.

The word "*Steganography*" is of Greek origin and means *" ... or hidden writing"*. Its ancient origins can be traced back to 440 BC. Generally, a steganographic message will appear to be something else: a picture, an article, a shopping list, or some other message. This … is the *covertext*. For instance, a message may be hidden by using invisible ink between … of innocuous documents.

The advantage of steganography over cryptography alone is that messages do not attract attention to themselves, to messengers, or to

recipients. An unhidden coded message, no matter how unbreakable it is, will arouse … and may in itself be incriminating, as in countries where encryption is ….

Steganography used in electronic communication includes steganographic coding inside of …, such as an MP3 file, or a protocol, such as UDP.

11. Translate the following passage into Russian.

Like many security tools, steganography can be used for a variety of reasons, some good, some not so good. Legitimate purposes can include things like watermarking images for reasons such as copyright protection. Digital watermarks (also known as fingerprinting, significant especially in copyrighting material) are similar to steganography in that they are overlaid in files, which appear to be part of the original file and are thus not easily detectable by the average person. Steganography can also be used as a way to make a substitute for a one-way hash value (where you take a variable length input and create a static length output string to verify that no changes have been made to the original variable length input). Further, steganography can be used to tag notes to online images (like post-it notes attached to paper files). Finally, steganography can be used to maintain the confidentiality of valuable information, to protect the data from possible sabotage, theft, or unauthorized viewing.

12. Translate the following passage into English.

В настоящее время появилось новое направление в области защиты информации — компьютерная стеганография. Учитывая естественные неточности устройств оцифровки и избыточность аналогового видео- или аудиосигнала, методы компьютерной

стеганографии позволяют скрывать сообщения в компьютерных файлах и потоках данных. Причем, в отличие от криптографии, данные методы скрывают сам факт передачи информации. Сокрытие сообщения методами стеганографии значительно снижает вероятность обнаружения самого факта передачи сообщения, при этом шифрование сообщения обеспечивает его конфиденциальность в случае обнаружения. В настоящее время можно выделить четыре тесно связанных между направления приложения стеганографии:

- защита конфиденциальной информации от несанкционированного доступа;
- преодоление систем мониторинга и управления сетевыми ресурсами;
- камуфлирование программного обеспечения;
- защита авторского права на некоторые виды интеллектуальной собственности.

13. Scan the text and point out its main ideas. Write the abstract of the text (See Appendix 2).

Text 2.

Null Ciphers

Historically, null ciphers are a way to hide a message in another without the use of a complicated algorithm. One of the simplest null ciphers is shown in the classic examples below:

PRESIDENT'S EMBARGO RULING SHOULD HAVE IMMEDIATE NOTICE. GRAVE SITUATION AFFECTING INTERNATIONAL LAW. STATEMENT FORESHADOWS RUIN OF MANY NEUTRALS. YELLOW JOURNALS UNIFYING NATIONAL EXCITEMENT IMMENSELY.

APPARENTLY NEUTRAL'S PROTEST IS THOROUGHLY DISCOUNTED AND IGNORED. ISMAN HARD HIT. BLOCKADE ISSUE AFFECTS PRETEXT FOR EMBARGO ON BYPRODUCTS, EJECTING SUETS AND VEGETABLE OILS.

The German Embassy in Washington, DC, sent these messages in telegrams to their headquarters in Berlin during World War I (Kahn 1996). Reading the first character of every word in the first message or the second character of every word in the second message will yield the following hidden text:

PERSHING SAILS FROM N.Y. JUNE 1

On the Internet, spam is a potential carrier medium for hidden messages. Consider the following:

Dear Friend, This letter was specially selected to be sent to you! We will comply with all removal requests! This mail is being sent in compliance with Senate bill 1621; Title 5; Section 303! Do NOT confuse us with Internet scam artists. Why work for somebody else when you can become rich within 38 days! Have you ever noticed the baby boomers are more demanding than their parents & more people than ever are surfing the web! Well, now is your chance to capitalize on this! WE will help YOU sell more & SELL MORE. You can begin at absolutely no cost to you! But don't believe us! Ms Anderson who resides in Missouri tried us and says "My only problem now is where to park all my cars". This mail is being sent in compliance with Senate bill 2116, Title 3 ; Section 306!....

This message looks like typical spam, which is generally ignored and discarded. This message was created at spam mimic, a Website that converts a short text message into a text block that looks like spam using a grammar-based mimicry idea first proposed by Peter Wayner. The reader will learn nothing by looking at the word spacing or misspellings in the message. The zeros and ones are encoded by the choice of the words. The hidden message in the spam carrier above is: **Meet at Main and Willard at 8:30.**

Special tools or skills to hide messages in digital files using variances of a null cipher are not necessary. An image or text block can be hidden under another image in a PowerPoint file, for example. Messages

can be hidden in the properties of a Word file. Messages can be hidden in comments in Web pages or in other formatting vagaries that are ignored by browsers. Text can be hidden as line art in a document by putting the text in the same color as the background and placing another drawing in the foreground. The recipient could retrieve the hidden text by changing its color. These are all decidedly low-tech mechanisms, but they can be very effective.

Digital Image and Audio

Many common digital steganography techniques employ graphical images or audio files as the carrier medium. It is instructive, then, to review image and audio encoding before discussing how steganography and steganalysis works with these carriers.

Figure 1 shows the RGB color cube, a common means with which to represent a given color by the relative intensity of its three component colors—red, green, and blue—each with their own axis (more Crayons 2003). The absence of all colors yields black, shown as the intersection of the zero point of the three-color axes. The mixture of 100 percent red, 100 percent blue, and the absence of green form magenta; cyan is 100 percent green and 100 percent blue without any red; and 100 percent green and 100 percent red with no blue combine to form yellow. White is the presence of all three colors.

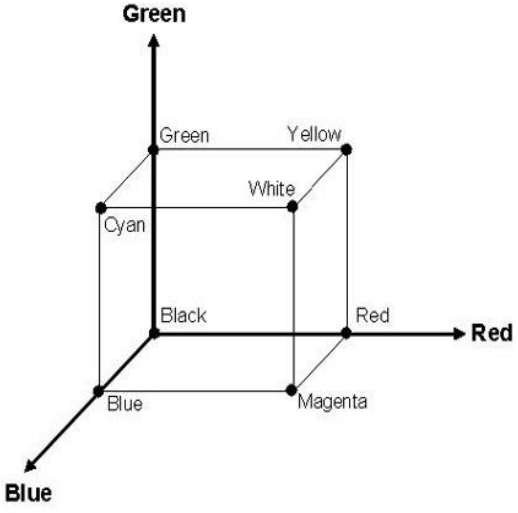


Figure 1. The RGB Color Cube

Most digital image applications today support 24-bit true color, where each picture element (pixel) is encoded in

24 bits, comprising the three RGB bytes as described above. Other applications encode color using eight bits/pix. These schemes also use 24-bit true color but employ a palette that specifies which colors are used in the image. Each pix is encoded in eight bits, where the value points to a 24-bit color entry in the palette. This method limits the unique number of colors in a given image to 256 (2^8).

The choice color encoding obviously affects image size. A 640 X 480 pixel image using eight-bit color would occupy approximately 307 KB (640 X 480 = 307,200 bytes), whereas a 1400 X 1050 pix image using 24-bit true color would require 4.4 MB (1400 X 1050 X 3 = 4,410,000 bytes).

Color palettes and eight-bit color are commonly used with Graphics Interchange Format (GIF) and Bitmap (BMP) image formats. GIF and BMP are generally considered to offer lossless compression because the image recovered after encoding and compression is bit-for-bit identical to the original image.

The Joint Photographic Experts Group (JPEG) image format uses discrete cosine transforms rather than a pix-by-pix encoding. In JPEG, the image is divided into 8 X 8 blocks for each separate color component. The goal is to find blocks where the amount of change in the pixel values (the energy) is low. If the energy level is too high, the block is subdivided into 8 X 8 subblocks until the energy level is low enough. Each 8 X 8 block (or subblock) is transformed into 64 discrete cosine transforms coefficients that approximate the luminance (brightness, darkness, and contrast) and chrominance (color) of that portion of the image. JPEG is generally considered to be lossy compression because the image recovered from the

compressed JPEG file is a close approximation of, but not identical to, the original.

Audio encoding involves converting an analog signal to a bit stream. Analog sound—voice and music—is represented by sine waves of different frequencies. The human ear can hear frequencies nominally in the range of 20-20,000 cycles/second (Hertz or Hz). Sound is analog, meaning that it is a continuous signal. Storing the sound digitally requires that the continuous sound wave be converted to a set of samples that can be represented by a sequence of zeros and ones.

Analog-to-digital conversion is accomplished by sampling the analog signal (with a microphone or other audio detector) and converting those samples to voltage levels. The voltage or signal level is then converted to a numeric value using a scheme called pulse code modulation. The device that performs this conversion is called a coder-decoder or codec.

Pulse code modulation provides only an approximation of the original analog signal, as shown in Figure 2. If the analog sound level is measured at a 4.86 level, for example, it would be converted to a five in pulse code modulation. This is called quantization error. Different audio applications define a different number of pulse code modulation levels so that this "error" is nearly undetectable by the human ear. The telephone network converts each voice sample to an eight-bit value (0-255), whereas music applications generally use 16-bit values (0-65,535).

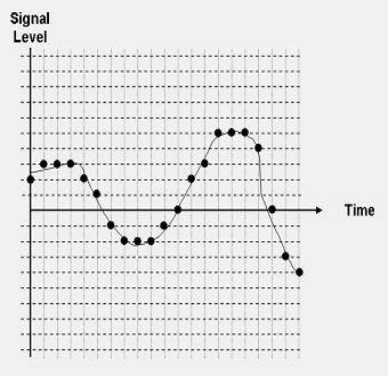


Figure 2. Simple Pulse Code Modulation

Analog signals need to be sampled at a rate of twice the highest frequency component of the signal so that the original can be correctly reproduced from the samples alone. In the telephone network, the human voice is carried in a frequency band 0-4000 Hz; therefore, voice is sampled 8,000 times per second (an 8 kHz sampling rate). Music audio applications assume the full spectrum of the human ear and generally use a 44.1 kHz sampling rate.

The bit rate of uncompressed music can be easily calculated from the sampling rate (44.1 kHz), pulse code modulation resolution (16 bits), and number of sound channels (two) to be 1,411,200 bits per second. This would suggest that a one-minute audio file (uncompressed) would occupy 10.6 MB (1,411,200*60/8 = 10,584,000). Audio files are, in fact, made smaller by using a variety of compression techniques. One obvious method is to reduce the number of channels to one or to reduce the sampling rate. Other codecs use proprietary compression schemes. All of these solutions reduce the quality of the sound.

14. Grammar. Modal Verbs. See Grammar reference.

Grammar tasks

Task A. State the function of the following modal verbs.

1. Electronic Signatures can come in many forms.
2. The single-photon source and the detectors must be connected by a “quantum channel”.
3. Two forms of attack might be carried out.
4. A DMBS application may consist of one or more executable images and one or more data files.

5. High-quality signatures can offer authentication, integrity and non-repudation.
6. Could you help us?
7. Shall we stop working over this project?
8. I'm sure you should continue your research.
9. It must have been the developed algorithm we hadn't met yet.
10. We believe our research group will be able to finish work in time.

Task B. Paraphrase the following sentences using the modal verbs given below.

1. I'm sure the paper is somewhere in the office. (must)
2. I think you are not working hard. (should)
3. I need this job! (must)
4. Perhaps our colleagues will come in time. It depends on the traffic. (might)
5. I'm sure the analysis is not ready. (can)
6. I think you don't pay proper attention to the questions of security. (should)
7. It is forbidden to write your password anywhere! (must)
8. If you don/t know how to solve this problem, ask your colleagues to help you. (should)
9. The failure of the security system is not his fault. I'm sure in it. (can)

Task C. Write sentences using modal verbs and the following words. Comment on the modal verbs used in the sentences.

1. The idea/machine/generate speech/be discussed/for about 50 years.
2. The vulnerability analysis/take/five work days.
3. Employee/change/passwords.

4. I/help you/with the project?
5. Excuse me! You/explain this message for me?
6. While designing a network, consider how other components of its perimeter (intrusion detection systems, routers, and VPNs) / influence the security of infrastructure.
7. Block encryption algorithms / be used in a number of different modes, such as “electronic code book” and “cipher block chaining”.
8. Worms are programs that / run independently and travel from machine to machine across network connections.

15. Writing.

Write an abstract of the material you’d like to present at the conference (see Appendix 2).

16. Communication.

Find positive and negative examples of applying steganography in the life of the modern society.

Make a presentation to illustrate the facts you’ve found.

Prepare the report for the group conference and be ready to discuss it.

Unit 6. QUANTUM CRYPTOGRAPHY.

Pronunciation

Make sure you pronounce the following words properly:

quantum ['kwɔntəm]	qubit [kju:bɪt]
eavesdrop ['i:vzdrɔp]	mechanics [mɪ'kænɪks]
vibrate [vaɪ'breɪt]	angle ['æŋgl]

vibration [vaɪ'breɪʃən]	discrepancy [dɪs'krepənsɪ]

Memorize the terms

1. Read the following terms and their definitions and memorize them:

be a bit off – be switched over, changed a bit

be bugged – be overheard

be on the lunatic fringe – be considered of minor importance, be ignored

discrepancy – difference, diversity

Eavesdrop – overhear, intercept

expand on an idea – study and speak in detail about an idea

insecure channel – unprotected channel that can be easily eavesdropped

measure – scale, determine

prearranged code – discussed beforehand

random result – probabilistic, patternless choice

2. Match the synonyms.

allow through	ruin
discrepancy	truncate
unauthorized	sequence
string	let pass
discard	difference
collapse	not having legal access

Reading

3. Pre-reading task.

Texts

What do you know about quantum cryptography and its application?

Comment on the efficiency of the quantum cryptography methods.

Can you name scientists and laboratories that conduct research in this sphere in Russia and abroad?

4. Text 1. Quantum cryptography. Find in the text the description of the phenomena of quantum mechanics.

Quantum cryptography is another kind of cryptography in this world. With it, you can create a communication channel where it is impossible to eavesdrop without disturbing the transmission. The laws of physics secure this quantum channel: even if the eavesdropper can do whatever he wants, even if the eavesdropper has unlimited computing power. Charles Bennett, Gilles Brassard, Claude Crepeau and others have expanded on this idea, describing quantum key distribution.

According to quantum mechanics, particles don't actually exist in any single place. They exist in several places at once, with probabilities of being in different places if someone looks. However, it isn't until a scientist comes along and measures the particle that it "collapses" into a single location. But you can't measure every aspect (for example, position and speed) of a particle at the same time. If you measure one of those two quantities, the very act of measuring it destroys any possibility of measuring the other quantity. The quantum world has a fundamental uncertainty and there's no way to avoid it.

That uncertainty can be used to generate a secret key. As they travel, photons vibrate in some direction; up and down, left to right or more likely at some angle. Normal sunlight is unpolarized; the photons vibrate every which way. When a large group of photons vibrate in the same direction they are *polarized.* Polarization filters allow only photons that are polarized in a certain direction through; the rest are blocked. For

example, a horizontal polarization filter only allows horizontally polarized photons through. Turn that filter 90 degrees, and only vertically polarized photons can come through.

Let's say you have a pulse of horizontally polarized photons. If they try to pass through a horizontally polarized filter, they all get through. Slowly turn that filter 90 degrees; the number of photons getting through gets smaller and smaller, until none gets through. You'd think that turning the filter just a little will block all the photons, since the photons are horizontally polarized. But in quantum mechanics, each particle has a probability of suddenly switching its polarization to match the filter. If the angle is a little bit off, it has a high probability. If the angle is 90 degrees off, it has zero probability. And if the angle is 45 degrees off, it has a 50 percent probability of passing through the filter.

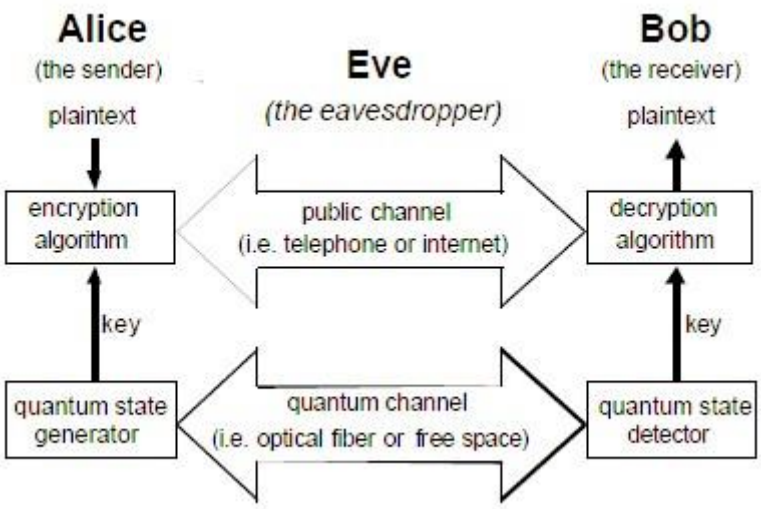
5. Answer the following questions.

What laws of physics is quantum cryptography based on?

Why can't you measure every aspect of a particle at the same time?

How do polarization filters work?

How can the laws of quantum mechanics be used in cryptography? Base on the diagram below.



6. Mark the following statements true or false. Correct the false statements.

1. The communication channel can be protected from the eavesdropper by the laws of physics.

2. No eavesdropper can intercept the transmission protected by quantum cryptography.

3. All characteristics of particles as studied by quantum mechanics can be easily measured.

4. Polarization filters let polarized photons pass through the communication channel in any direction.

5. If we turn the vertically polarized filter 90 degrees the horizontally polarized photons won't get through.

6. You can learn the polarization only if you measure it in the basis it is polarized.

7. If we turn the horizontally polarized filter 30 degrees the vertically polarized photons will get through.

8. In quantum mechanics particles can change the polarization to get through the filter.

9. Quantum cryptography is still theoretical.

10. According to quantum mechanics particles can adapt to the polarization of the filter.

Vocabulary tasks

7. Give English equivalents of the following Russian words and words combinations.

Неопределенность, передача (информации), возможность, под углом, в определенном направлении, избежать, проходить сквозь что-либо.

8. Give Russian equivalents of the following English words and words combinations.

Expand, disturb the transmission, over an insecure channel, discrepancy, the parity of subsets, discard, recover the bits.

9. Make the word combinations.

1. polarization	a) channel
2. rectilinear	b) of subsets
3. the parity	c) bit commitment
4. communication	d) on the idea
5. quantum	e) channel
6. random	f) polarization
7. expand	g) code
8. insecure	h) filter
9. pre-arranged	i) polarization
10. diagonal	j) result

10. Complete the text using the terms and word combinations given below.

An eavesdropper, guarantees, without disturbing, vulnerable, access

It is impossible to obtain information about physical system … it in a random, uncontrollable way. This fundamental quantum-mechanical law … the security of Quantum Key Exchange (QKE) protocols. QKE protocols such as BB84 have been proved to be secure under the assumption that the known laws of physics hold. Given this assumption, QKE is unconditionally secure, i.e. secure even in the presence of … with unlimited computational power.

QKE requires that the parties have … to an authentic channel. Any QKE protocol that does not fulfill this requirement is … to a man-in-the middle attack.

2. Render the following passage in Russian.

Quantum Channels.

The single-photon source and the detectors must be connected by a "quantum channel". Such a channel is not especially quantum, except that it is intended to carry information encoded in individual quantum systems. The idea is that the information is coded in a physical system only once, in contrast to classical communication, in which many photons carry the same information. Note, that the present-day limit for fiber-based classical optical communication is already down to a few tens of photons, although in practice one usually uses many more.

Individual quantum systems are usually two-level systems, called qubits. During their propagation they must be protected from environmental noise. Here "environment" refers to everything outside the

degree of freedom used for the encoding, which is not necessarily outside the physical system. If, for example, the information is encoded in the polarization state, then the optical frequencies of the photon are part of the environment. Hence coupling between the polarization and the optical frequency has to be mastered. Moreover, the sender of the qubits should avoid any correlation between the polarization and the spectrum of the photons.

13. Translate into English.

1. Квантово-криптографические системы - это побочный продукт разрабатываемого в настоящее время так называемого квантового компьютера.

2. Основная причина бурных исследований в области квантовых компьютеров – это естественный параллелизм квантовых вычислений.

3. Например, если квантовая память состоит из двух кубитов, то мы параллельно работаем со всеми ее возможными состояниями: 00, 01, 10, 11.

4. Бурное развитие квантовых технологий и волоконно-оптических линий связи привело к появлению квантово-криптографических систем.

5. В квантово-криптографическом аппарате применим принцип неопределенности Гейзенберга, согласно которому попытка произвести измерения в квантовой системе вносит в нее нарушения, и полученная в результате такого измерения информация определяется принимаемой стороной как дезинформация.

6. Итак, две конечных цели квантовой (как и классической) криптографии:

1) обеспечить отправителю и адресату защищенный канал обмена информацией;

2) обеспечить механизм проверки секретности такого обмена.

7. Секретным и абсолютно защищенным, в принципе, можно сделать любой канал передачи информации.

8. Достаточно лишь чтоб обмен шел сообщениями, зашифрованными криптостойким шифром и качественным секретным ключом.

9. Секретным считаем ключ, известный лишь отправителю и адресату.

10. Качественный ключ представляет собой абсолютно случайную последовательность 0 и 1.

14. Read the text and outline the process of secret key generation.

Text 2.

Secret Key Generation.

Polarization can be measured in any basis: two directions at right angles. An example basis is rectilinear: horizontal and vertical. Another is diagonal: left-diagonal and right-diagonal. If a photon pulse is polarized in a given basis and you measure it in the same basis, you learn the polarization. If you measure it in the wrong basis, you get a random result. We're going to use this property to generate a secret key:

For example: Alice and Bob are users, and Eve is an eavesdropper.

1) Alice sends Bob a string of photon pulses. Each of the pulses is randomly polarized in one of four directions: horizontal, vertical, left-diagonal, and right-diagonal.

2) Bob has a polarization detector. He can set his detector to measure rectilinear polarization or he can set his detector to measure diagonal polarization. He can't do both; quantum mechanics won't let him. Measuring one destroys any possibility of measuring the other.

Now, when Bob sets his detector correctly, he will record the correct polarization. If he sets his detector to measure rectilinear polarization and the pulse is polarized rectilinearly, he will learn which way Alice polarized the photon. If he sets his detector to measure diagonal polarization and the pulse is polarized rectilinearly, he will get a random measurement. He won't know the difference.

3) Bob tells Alice, over an insecure channel, what settings he used.

4) Alice tells Bob which settings were correct.

5) Alice and Bob keep only those polarizations that were correctly measured.

Using a prearranged code, Alice and Bob each translate those polarization measurements into bits. For example, horizontal and left-diagonal might equal one, and vertical and right-diagonal might equal zero.

So, Alice and Bob have generated bits as many as they like. On the average, Bob will guess the correct setting 50 percent of the time, so Alice has to send *2n* photon pulses to generate *n* bits. They can use these bits as a secret key for a symmetric algorithm or they can guarantee perfect secrecy and generate enough bits for a one-time pad.

The really cool thing is that Eve cannot eavesdrop. Just like Bob, she has to guess which type of polarization to measure; and like Bob, half of her guesses will be wrong. Since wrong guesses change the polarization of the photons, she can't help introducing errors in the pulses as she eavesdrops. If she does, Alice and Bob will end up with different bit strings.

6) So, Alice and Bob compare a few bits in their strings. If there are discrepancies, they know they are being bugged. If there are none, they discard the bits they used for comparison and use the rest.

Improvement to this protocol allows Alice and Bob to use their bits even in the presence of Eve. They could compare only the parity of subsets of the bits. Then, if no differences are found, they only have to discard one bit of the subset. This detects eavesdropping with only a 50 percent probability, but if they do this with *n* different subsets Eve's probability of eavesdropping without detection is only 1 in 2".

There's no such thing as passive eavesdropping in the quantum world. If Eve tries to recover all the bits, she will necessarily break the communication.

Vocabulary and Grammar 1-6. Revision.

I. Put the words in the correct order. The first word is underlined.

1. scientists, of, <u>the method</u>, frequency, using, a code, discovered, Arabic, breaking, analysis, by, was

2. process, input, <u>the results</u>, are, of, valuable, the evaluation, to, the accreditation

3. will, evaluation, the CC, between, independent, permit , the results, comparability, of, security

4. began, hackers, in 1990, the government, campaign, to crackdown, nationwide

5. to remain, developments, cryptology, an area, interesting, promises, of

6. by, evaluated, Protection Profile, be, applying, can, the APE criteria

7. aspects, algorithms, combine, secure and fast, hybrid cryptosystems, are, of, and, symmetric, public-key, and

8. any, change, in, does, transposition (or permutation), not, bits, the plaintext

II. Complete the sentences using the words given below.

Block ciphers, require, were hidden, judgments, to recover, inspection, a protocol, certification, jargon code, a set.

1. The certification process is the independent _____ of the results of the evaluation leading to the production of the final certificate or approval.
2. The CC is presented as _____ of distinct but related parts.
3. The evaluation scheme, methodology and _____ processes are the responsibility of evaluation authorities that run evaluation scheme.
4. Many of the evaluation criteria _____ the application of expert judgements and background knowledge for which consistency is more difficult to achieve.

5. The CC contains criteria to be used by evaluators when forming _____ about the conformance of TOEs to the security requirements.
6. In ancient times, messages _____ on the back of wax writing tables.
7. A method of encryption is only secure if even with this complete access, the eavesdropper is still unable _____ the original plaintext from the ciphertext.
8. Kerberos is _____ for single sign-on and authenticating users against a central authentication and key distribution server.
9. _____ like DES are intended to be very hard to break.
10. _____ , as the name suggests, uses language that is understood by a group of people but is meaningless to others.

III. Match the lines.

1. assurance	a) host
2. trial	b) analysis
3. covert	c) cipher
4. estimate	d) text
5. vulnerability	e) measures
6. carrier	f) encipherment
7. integrity	g) aids
8. automated	h) protection
9. communicating	i) communication
10. null	j) the risk

IV. Put the verbs in brackets in the correct form Active or Passive.

1. Back in the 90-s, Anti-virus researchers first (fight back) by creating special detection routines designed to catch each polymorphic virus, one by one.
6. By hand, line by line, they (write) special programs.
7. W.F.Friedman's monograph «The Index of Coincidence and its Application in Cryptography» (appear) in 1918.
8. US Army and Navy (work) entirely in secret, when their specialists (begin) making fundamental advances in cryptography.
9. H.Feistel, who earlier (work) on identification friend or foe devices for the Air Force, (change) the sphere of his scientific interests.
10. The earliest ciphers (involve) only vowel substitution.
11. French cryptographer of the 16th century B. de Vigenere (produce) a more sophisticated autokey cipher, but for the last 400 years people (attach) his name to a weaker cipher.
12. Ch.Wheatstone (initiate) the usage of electromagnets in electric generators.
13. Codes, in which all combinations (have) identical length, (name) uniform.
14. There are the cases when the information (transfer) not only from one subscriber to another, but also in the opposite direction.
15. Memory cards (not process) the information.
16. Message-digest algorithms (develop) in 1989 – 1991.
17. The global network Internet (take) a significant place for the last 50 years.
18. The traditional cryptosystems (design) so that they (accept) only identical keys which (use) for encryption and decryption.

19. Cryptographic key (can/hide) within the user's biometric template.
20. If a photon pulse (measure) in the wrong basis, a random result (get).

V. Give definitions of the following terms.

Availability, hill climbing algorithm, plaintext, optional authentication of the client, reduce risk, semagram, ciphertext-only solution, be a bit off, integrity, access point.

VI. Translate into Russian.

1. Part 2 of the CC, security functional requirements, establishes a set of functional components as a standard way of expressing the functional requirements for TOEs.
2. Unauthorised access to the database can be carried out in a form of passive attacks (e.g. monitoring of network).
3. To keep your PC protected from new viruses, Trojan horses and other malicious software flying around the Internet, the anti-virus program needs to download regular updates from the manufacturer.
4. The process begins with a characterization of the facility including identification of the undesired events and the respective critical assets.
5. In the last few decades cryptographic algorithms, being mathematical by nature, have become sufficiently advanced that they can only be handled by computers.
6. A well-designed cipher will not offer a simple opportunity to try different possibilities to find partial information about the key.
7. Although the term steganography was only coined at the end of the 15th century, the use of steganography dates back several millennia.

8. According to quantum mechanics, particles don't actually exist in any single place.
9. The evaluation results may help consumers to determine whether the IT product or system is secure enough for their intended application.
10. The converted unit record equipment (punched card machines) compared Japanese code messages to one another at various displacements to find messages with overlapping superencipherment groups.

VII. Translate into English.

1. Термин «угроза» обозначает события, которые могут иметь неблагоприятные последствия.
2. Управление информационными рисками – сложный процесс, требующий постоянного анализа рисков.
3. Вопросы безопасности должны быть неотъемлемой частью разработки компьютерных приложений.
4. Хорошо спланированная и выполненная оценка риска должна эффективно определять и измерять последствия широкого спектра угроз.
5. Количественная и качественная метрические схемы, применяемые для измерения элементов риска, были впервые разработаны Национальным бюро стандартов.
6. В традиционной криптографии отправитель и получатель сообщения используют один и тот же секретный ключ для зашифрования и расшифрования.
7. Было предпринято несколько попыток определить наличие стеганографических объектов в Интернете.

8. Этот поточный шифр используется для защиты телефонных разговоров в большинстве европейских стран и США.
9. DES широко используется уже 20 лет.
10. К анализу риска продолжают относиться скептически.

VIII. Communication

Role play. Work over the role you've chosen. Be ready to take part in the conference.

International Conference on Computer Security and Privacy.

Chairman. *Study the topics and summaries of the reports. Think of the agenda, your comments and possible questions.*

Secretary. *Be ready to make notes of the reports, questions and answers.*

Members of the conference. *Be ready to present your report using diagrams and hand-out. Take part in the discussion of the reports.*

Journalists. *Study the topics and summaries of the reports. Listen to the presentation of the reports. Be ready to ask questions.*

IX. Writing

Write an abstract of your report for the conference to be presented in the group (see Appendix 2).

Unit 7. MEANS AND METHODS FOR THE INFORMATION PROTECTION IN THE INTERNET

Pronunciation

Make sure you pronounce the following words properly:

penetration [ˌpenɪ'treɪʃən]	emphasize ['emfəsaɪz]

intrusion [ɪn'tru:ʒən]	legislative ['ledʒɪslətɪv]
vulnerable ['vʌlnərəbl]	legal ['li:gəl]
access ['ækses]	virus ['vaɪərəs]
maintenance ['meɪntənəns]	purpose ['pə:pəs]
reliance [rɪ'laɪəns]	enterprise ['entəpraɪz]

Memorize the terms

1. Read the following terms and their definitions and memorize them:

embedding of a program – building into a program

penetration – illegal, unauthorized access

shortcoming (of an approach) – disadvantage, weak point

smart-attack – a kind of specially directed generated attack

take a significant place – be of great importance

unauthorized user – user that tries to get access illegally, without any permission or license

vulnerable network component – network component that is subject to risk

2. Match the following words with their synonyms:

penetration	reliable, strong
reveal	keep form
intrusion	consider, take into consideration
prevent	intrusion
take into account	breaking the security system, penetration

proof (algorithm)	detect
integrity	safety

Reading

3. Pre-reading task.

Dwell on the role and the spheres of application of Internet in the life of the modern society.

What types of information threats in Internet do you know?

What are the “weak points” in the information protection of the Internet?

What means of information protection can you name?

Which means would you recommend?

4. Decide where the following sentences go in the text.

_ *The examples of software protection tools are: firewalls, cryptographic program means, authenticating means, means for the vulnerable network components definition and protection.*

_ *The access of organization to the global network INTERNET essentially increases its functioning effectiveness and opens a set of new opportunities.*

_ *On the other hand, the organization should provide the creation of information resources protecting system to prevent an access of unauthorized users, who may use, modify or destroy important information.*

_ *The hardware tools are the set of hardware means intended to the data enciphering and to the protection from viruses.*

Text 1. The information protection in the global network internet.

The global network INTERNET takes a significant place in a life of the modern society. Nowadays the INTERNET covers many spheres of

activities, in particular, such branches as information technologies, commercial operations, information interchange, bank business, education etc. Regardless of its specifics, the information protecting system for global networks is a part of general security complex directed on information safety assurance. The information protection is the complex of means directed on information safety assuring. In practice it should include maintenance of integrity, availability, confidentiality of the information and resources used for data input, saving, processing and transfer. The complex character of this problem emphasizes that for its solution the combination of legislative, organizational and software-hardware measures should be realized.

The main threats to the information safety in the INTERNET.

The unauthorized access (UAA) in the INTERNET can be performed, in particular, using the following actions:

– penetration into network with the purpose of reading the confidential information;

– penetration into network with the purpose of updating or destroying the existing information;

– embedding of the programs - viruses, which will disorganize the network functions or perform all above mentioned actions;

– destroying of the INTERNET-servers functioning or local computers connected to the INTERNET.

All these actions can be realized separately or in any combination.

Let's list some examples of the unauthorized intrusions in the INTERNET: smart attacks of the INTERNET-viruses, the Troyan

programs that assemble the secured information from WEB-pages, destroy the servers functioning etc.

The protection from unauthorized access in the INTERNET.

Every information protecting mean is directed to the certain type of safety threats, and realizes the protection against specific types of the unauthorized access. There are program and hardware protecting tools.

The software protecting tools are program complexes intended to reveal and to prevent the possible UAA threats.

The examples of hardware tools are: cryptographic electronic boards and hardware complexes-anti-viruses.

Nowadays the simple approaches to the protection system organization are the most widespread, such as the systems for protection from the unauthorized users' access. These systems are rather reliable however they do not offer the required flexibility. They are based on the various tools for protection assurance, for example, the tools that permit the data transfer only to those users who possess the certain addresses of network protocol IP, tools that deny the direct users access to the INTERNET resources and local networks. The shortcomings of this approach consist in narrowness of the solved problem: to prevent access of the unauthorized users to the various local networks. The similar protection is used for access prevention of the certain users of the local network (for example, corporate network of the enterprise) to the all INTERNET resources, except for electronic mail. The principle of this protection method is the following: the protection of the local information and decreasing of external channels traffic. However users and providers of the INTERNET services are more concerned in maintaining of general

safety of network, in particular, the confidentiality of the information of the sender and receiver, and the absolute reliance is necessary for the providers and users that on the other end of the communication channel is the legal user.

5. Answer the following questions.

What are the demerits of using Internet?

What types of information threats in Internet are mentioned in the text?

What are the examples of such threats?

What are the most widespread means for information protection?

What are the main directions of the protection activities for the users and providers of the Internet services?

How can the main threats to the information safety in the INTERNET be classified?

6. Mark the following statements true or false. Correct the false statements.

1. Information safety assurance involves keeping all operations with data protected.
2. Software-hardware measures are enough to solve the problem of UAA.
3. The examples of software protection tools are cryptographic electronic boards.
4. An example of hardware tools is a hardware complex-anti-virus.
5. Nowadays the complicated approaches to the protection system organization are the most often used.
6. The access of organization to the global network INTERNET essentially increases its functioning effectiveness.

7. The information protection should include maintenance of integrity, availability, confidentiality of the information and resources used for data input, saving, processing and transfer.
8. The Troyan programs collect the secured information from WEB-pages.
9. The systems for protection from the unauthorized users' access just prevent access of the unauthorized users to the various local networks.
10. There are some general protecting means that can work against all threats.

Vocabulary tasks

7. Give as many word combinations as possible and translate them.

Access, system, tools, protocol, network.

8. Form different parts of speech and translate them.

Verb	**Noun**
expand	
intend	
	intrusion
	direction
allow	
Noun	**Adjective**
	complex
reliability	
	digit

9. Give your definitions of the following terms.

Smart attack, flexibility of a system, proof algorithm, shortcoming

10. Make the word combinations.

1. take	a) the required flexibility
2. proof	b) complex
3. shortcomings	c) of a program
4. an access	d) a significant place
5. unauthorized	e) assurance
6. increase	f) of an approach
7. offer	g) algorithm
8. embedding	h) functioning effectiveness
9. general security	i) user
10. information safety	j) of an organization

11. Complete the text using the terms and word combinations given below.

Change, run together, operating system, to malfunction, floppy discs, follow, to attach themselves

Virus is a self-duplicating computer program that interferes with a computer's hardware or …. Like any other computer program, a virus must be located in the computer's memory, and the computer must then … the virus's instructions. These instructions are called the payload of the virus. The payload may destroy or … data files, display an irrelevant or unwanted message, or cause the operating system ….

Infection is much more frequent in PCs than in professional mainframe systems because programs on PCs are exchanged primarily by means of … , e-mail or over unregulated computer networks.

Some viruses have the ability … to legitimate programs. This attachment may occur when the legitimate program is created, opened or modified. The virus is … with the program.

12. Render in Russian the following passage.

Hosts attached to a network - particularly the worldwide Internet - are exposed to a wider range of security threats than are unconnected hosts. Network security reduces the risks of connecting to a network. But by nature, network access and computer security work at cross-purposes. A network is a data highway designed to increase access to computer systems, while security is designed to control access. Providing network security is a balancing act between open access and security.

The highway analogy is very appropriate. Like a highway, the network provides equal access for all - welcome visitors as well as unwelcome intruders. At home, you provide security for your possessions by locking your house, not by blocking the streets. Likewise, network security generally means providing adequate security on individual host computers, not providing security directly on the network.

In very small towns, where people know each other, doors are often left unlocked. But in big cities, doors have deadbolts and chains. In the last decade, the Internet has grown from a small town of a few thousand users to a big city of millions of users. Just as the anonymity of a big city turns neighbors into strangers, the growth of the Internet has reduced the level of trust between network neighbors. The ever-increasing need for computer security is an unfortunate side effect. Growth, however, is not all bad. In the same way that a big city offers more choices and more services, the

expanded network provides increased services. For most of us, security consciousness is a small price to pay for network access.

Network break-ins have increased as the network has grown and become more impersonal, but it is easy to exaggerate the extent of these security breaches. Over-reacting to the threat of break-ins may hinder the way you use the network.

Common sense is the most appropriate tool that can be used to establish your security policy. Elaborate security schemes and mechanisms are impressive, and they do have their place, yet there is little point in investing money and time on an elaborate implementation scheme if the simple controls are forgotten.

13. Translate into English the following passage.

Система распознавания атак должна обеспечивать реализацию следующих функций:

- обнаружение подготовки к атаке;
- сборка пакетов;
- выявление типовых атак на основе базы сигнатур атак;
- выявление атак; отсутствующих в базе сигнатур, при помощи использования нейронной сети для анализа сетевого трафика;
- автоматическое осуществление ответной реакции системы в случае обнаружения атаки.

Средства моделирования атак также разрабатываются на основе архитектуры захвата пакетов WinPcap.

14. Scan the text and mark the sentences about the main disadvantage of using credit cards. Point out the ways to solve the problem mentioned in the text.

Text 2.

Credit Card Security.

This is the age of plastic money. It's not uncommon for the typical consumer in the western world to go weeks at a time without ever handling a coin or bill. Everything we need is available to us with the simple "swik-swik' sound of a credit card sliding through a reader.

The big question is: "How safe is all this plastic?"

Cash has its obvious benefits. When you buy a sandwich for $2.95 and you hand the cashier a $5 bill, you know you haven't been ripped off when he hands you $2.05 right then and there. But when you hand your card to a waitress at the local chain restaurant, how do you know she hasn't taken a moment to sneak into the office and copy your card number and signature?

In response to these issues, the big credit card companies have developed more secure ways to do business. MasterCard International and Visa got together and came up with a set of guidelines called the Payment Card Industry Data Security Standards. This is a list of 12 guidelines that imposes strict regulations on all transactions taking place between the card company and the merchants it trades with. While these standards have been in place since 2005, merchants are taking some time to catch up to them. However, in the past year there has been marked improvement, and both credit card companies have stepped up their tactics to the point where merchants may be experiencing losses of service if they do not fall in line soon.

Discover Card has responded to the pressure for more secure methods with its own program. They call it the Secure Online Account

Number program. Anytime you use your Discover card to purchase a product online, their program will generate a random account number to "stand-in" for the one on your card. You then send this number to the merchant in place of the real number. When the number is verified with Discover Card, it will link to your account and the purchase is charged to you. The benefit of this system is that the merchant never sees your true account number. Only you and Discover Card have access to it. Once the transaction is completed the randomly generated account number is no longer valid, so any attempts to use it result in denial.

A security method that online merchants are employing is the requirement of a shipping address that matches the billing address on your credit card. This is to guard against thieves who may steal your account number but will have no access to your billing address. This way, if your card is stolen, it can only be used to make purchases that will ship to your address. Any prospective thieves will have to pick up their orders from your mailbox, not something the average anonymity-seeking thief will want to do.

There are also third party systems in place for ensuring online credit card security. VeriSign's SSL (Secure Sockets Layer) technology is the leader in the field. VeriSign will give each merchant it conducts business with 2 "keys" (like coding alphabets), a public key and a private key. The public key is used to encrypt information, and the private key is used to decipher it. VeriSign's technology now offers this encryption in 128- to 256-bit encryption, which provides a nearly un-guessable number of possible combinations of codes.

15. Grammar. The Gerund. See Grammar Reference.

Grammar tasks

Task A. Translate the sentences into Russian. **State the functions of the gerund.**

I'm sure we should go on making the experiment. As well as devising the Playfair cipher Charles Wheatstone invented the Wheatstone bridge. One starts performing the encryption by locating the two letters from the plaintext into matrix. The other approach to concealing plaintext structure in the ciphertext involves using several different substitutional ciphers. It is the periodicity of the repeating key which leads to the weakness in this method. Decryption is simply the reverse of the encryption process using the same secret key. When decrypting a route cipher, the receiver simply enters the ciphertext into the agreed-upon matrix. For encrypting elements of a plaintext made up of more than a single letter only digraphs (two successive letters) have ever been used.

Task B. Find the gerund and the Complex Gerundial Constructions. Translate the sentences into Russian.

They announced that no one had chance of cracking the cipher. Wheatstone's inventing the cipher made development of substitution ciphers. They insisted on the encryption being made. It may be easier to remember this as the plaintext letters being at two corners of a rectangle. He succeeded in cryptoanalyzing running-key ciphers. The Greeks being the inventors of the first transpositional cipher wrote the first work "On the Defense of Fortifications". The first European manual on cryptography, consisting of a compilation of ciphers, was produced by Gabriele de Lavinde of Parma. Herbert Yardley organized and directed the US government's breaking of the codes during and after the First World War.

Task C. Translate the sentences into English.

1. Я не намерен здесь больше оставаться.
2. Извините за беспокойство.
3. Думаю, он способен справиться с этой работой.
4. Я всегда интересовался проблемой защиты от несанкционированного доступа в Интернете.
5. Проект имеет целью разработку политики безопасности Интернет.
6. Спасибо за помощь.
7. Вибрируя в одном направлении, фотоны поляризуются.
8. Мы знаем, что Томко предложил разрабатывать повторяющиеся ключи на основе биометрических данных.
9. Использование портативного шифрующего устройства позволяет защитить информацию, хранящуюся в компьютере.
10. После обнаружения вируса антивирусная программа удаляет его.
11. Существует много примеров вирусов, заражающих компьютерные программы.
12. Результатом этого анализа является определение уязвимости, которая может увеличить частоту или влияние угроз на целевую среду объекта.
13. Мы ждали завершения оценки безопасности.

16. Communication

You’re going to have a job interview. Get ready for it. Prepare your resume, CV and short video presentation. Point out your academic skills, work experience, career plans.

17. Writing. Resume. Read the variants of resume and write your own one. See Appendix 3.

Unit 8. INTRANET SECURITY

Pronunciation

Make sure you pronounce the following words properly:

iris ['aɪərɪs]	misconception [ˌmɪskən'sepʃən]
employee [ˌemplɔɪ'i:]	legacy ['leɡəsɪ]
guideline ['ɡaɪdlaɪn]	proprietary [prə'praɪətərɪ]
encompass [ɪn'kʌmpəs]	paramount ['pærəmaunt]

Memorize the terms

1. Read the following terms and their definitions and memorize them:

external risk - risk of breaking security outside, e.g. by unauthorized users not involved in the work of the enterprise

internal risk – risk of breaking security inside, e.g. by the staff of the enterprise

malware – software created by malicious users

one-time password – password that is used only once

outsourcing – transfer of some business functions or some parts of a business process of an enterprise to an eternal contractor

reusable password – password that is used several times without changing it

security breach – malicious actions directed to getting unauthorized access

security outsourcing – engaging outside resources for solving problems of information protection

2. Match the following words with their Russian equivalents.

Packet sniffing	блокирование слежения
Secure Sockets Layer	активный, упреждающий
dedicated private line	контроль сообщений, передаваемых по сети связи, с целью выявления конфиденциальной информации
intranet publishing guideline	частная сеть для специальных целей
blocking snooping	протокол безопасных соединений
proactive	руководство по пользованию корпоративной сетью

3. Match the following words with their synonyms.

repository	counteracting

misconception	outside
theft	ordinary
external	stealing
reactive	data storage
thin (client)	misunderstanding

Reading

4. Pre-reading task.

What is Intranet?

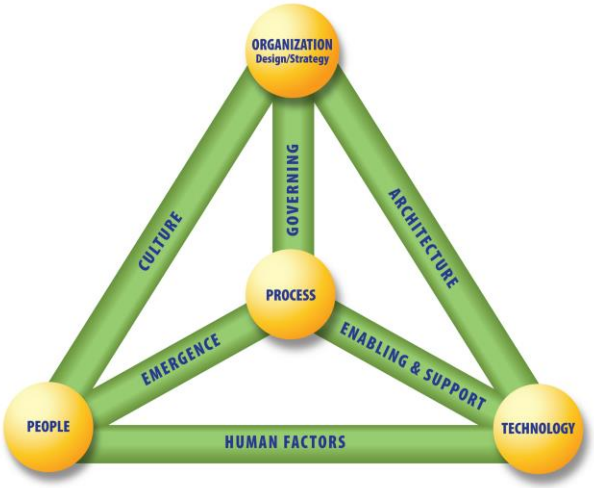
Why are intranets built?

Which advantages and disadvantages does building of intranets have?

5. Read the text and find out whether the following ideas are true, false or not discussed in it.

1. Few organizations use Intranets nowadays.
2. Intranets are used more often than Internet.
3. Intranets are secure unlike Internet.
4. One-time passwords are rather rarely used.
5. Reusable passwords are the main reason of intrusions.
6. Most security breaches in Intranet are committed by hackers.
7. Encryption is not used for protecting intranets.
8. In the report most attention is paid to the procedure of security staff employment.
9. Extranets contribute to the developing of E-commerce.
10. The report presented below underlines the necessity of cooperative activities aimed at intranets securing.

Text 1. Intranet Security



Intranets: An Emerging Business Resource. Intranets are revolutionizing the way organizations function. Internal Web servers have moved from being a repository for simple shared content to encompassing applications that interact with legacy systems. Unfortunately, these advantages also bring critical risks if the intranet is not properly secured. CTR's new report, Intranet Security, is designed to help information systems (IS) managers and other information security personnel work together to build secure corporate intranets. The report discusses the misconception that intranets are intrinsically more secure than Internet applications and explains why businesses must evaluate their risk level before implementing a security policy. Specific security tools and the future of intranets are also examined in detail.

Intranet Security: Internal and External Risks. CTR's Intranet Security report evaluates the internal and external risks related to intranets, including: data theft, viruses, Web server vandalism, client security, and reusable passwords. Reusable passwords act as the doorway for intruders in 72% of attacks. The report addresses the need for strong authentication methods, such as one-time passwords (OTP) and digital certificates. The report also explores the risks associated with providing remote intranet access. Virtual private networks (VPN's) provide a means to securely connect remote offices to the intranet. The technology behind VPN's is

examined, as well as the cost of providing access using VPN's versus leased lines. Because intranets are typically open to the entire company, the majority of security breaches are committed internally. The report discusses this issue and offers valuable information on how to protect your organization against internal security breaches.

*Intranet Security Solutions***.** Intranet Security offers an in-depth discussion of available intranet security products and technologies. Perhaps the most well-known measure for securing intranets is the use of firewalls. The report compares the different types of firewall products, describes the capabilities and limitations of firewalls, and offers a set of guidelines for successfully operating firewalls. Another key technology for securing intranets is encryption. The report assesses the need for encryption and offers an overview of important encryption concepts and technologies such as public key encryption, digital signatures, and the Secure Sockets Layer (SSL).

Developing an Intranet Security Policy. Developing an intranet security policy is the most important measure that organizations can take to improve their security. While existing security policies may address computing and network issues, intranet policies must cover such areas as intranet publishing guidelines and employee use of the Internet.

Future Trends in Intranet Security. Intranet Security includes a discussion of trends in the intranet security market, including all-in-one solutions, increased use of security outsourcing, and predictions that intranet security breaches will increase in the short-term as many organizations are reactive rather than proactive in implementing intranet security. One important, and very popular, trend in corporate intranets

involves making intranets available to third parties. Extended intranets, called extranets, allow customers and business partners' access to the intranet. This connection enables the use of technologies such as E-commerce. Intranets offer strategic advantages to businesses by creating a centralized knowledge base, enabling collaboration, and providing a standard interface to information across all hardware platforms. As intranets grow into trusted resources, relied on by employees and customers alike, the need to protect them becomes paramount. This new report from CTR includes the tools and information necessary to help ensure the protection and success of your corporate intranet.

6. Answer the following questions.

How can you characterize the kind of this text?

What is it made for?

What is the role of Intranets as business resource?

What are the risks of Intranet Security?

What are extranets?

How are they connected with E-commerce?

What means of intranet protection are mentioned in the text?

What are the ways and perspectives of developing an Intranet Security Policy?

Vocabulary tasks

7. Form different parts of speech and translate them.

Noun	**Adjective**
advantage	
	confidential
capability	

access	
value	
Noun	**Verb**
value	
	ensure
breach	

8. Give your definitions of the following terms.

Remote intranet access, security outsourcing, intranet publishing guideline, reactive, proactive, misconception.

9. Make the word combinations.

1. internal	a) password
2. retinal	b) breach
3. data	c) certificate
4. host	d) intranet access
5. Port	e) data
6. reusable	f) pattern
7. proprietary	g) risk
8. security	h) forwarding
9. remote	i) theft
10. digital	j) network

10. Give English equivalents of the following words and word combinations.

Взаимодействовать, защищать надлежащим образом, подробно рассматриваться, карта информации, обеспечивать, ряд инструкций, реагировать на что-либо, прогноз, доступный.

11. Give Russian equivalents of the following words and word combinations.

Shared content, encompassing applications, intrinsically, remote intranet access, leased line, security outsourcing, paramount.

12. Translate into Russian.

VPN can be a cost effective and secure way for corporations to provide users access to the corporate network and for remote networks to communicate with each other across the Internet. VPN connections are more cost-effective than dedicated private lines. Usually a VPN involves 2 parts: the protected or "inside" network, which provides physical and administrative security to protect the transmission; and a less trustworthy, "outside" network or segment (usually through the Internet). Generally, a firewall sits between a remote user's workstation or client and the host network or server. As the user's client establishes the communication with the firewall, the client may pass authentication data to an authentication service inside the perimeter. A known trusted person, sometimes only when using trusted devices, can be provided with appropriate security privileges to access resources not available to general users.

13. Complete the text by translating Russian phrases given in brackets.

(1 Мы представляем новый подход) to improving the security of passwords. In our approach, the legitimate user’s typing patterns (e.g., durations of keystrokes and latencies between keystrokes) (2 сочетаются с паролем пользователя) to generate a hardened password that is (3 несомненно более надежен) than conventional passwords alone. In addition, (4 наша схема автоматически

адаптируется к постепенным (периодическим) изменениям) in a user’s typing patterns while maintaining the same hardened password across multiple logins, for use in file encryption or other applications (5 для которых необходим долгосрочный секретный ключ). Using empirical data and a prototype implementation of our scheme, (6 мы подтверждаем) that our approach is viable (7 в практике, простоте использования, повышенной безопасности и исполнении).

14. Read the text and write the plan. Characterize briefly the types of VPNs.

Text 2.

Virtual private network.

A **virtual private network** (**VPN**) is a private communications network often used by companies or organizations to communicate confidentially over a public network. VPN traffic can be carried over a public networking infrastructure (e.g. the Internet) on top of standard protocols, or over a service provider's private network with a defined Service Level Agreement (SLA) between the VPN customer and the VPN service provider. A VPN can send data (e.g., voice, data or video, or a combination of these media) across secured and encrypted private channels between two points.

Authentication mechanism

VPN can be a cost effective and secure way for corporations to provide users access to the corporate network and for remote networks to communicate with each other across the Internet. VPN connections are more cost-effective than dedicated private lines. Usually a VPN involves 2 parts: the protected or "inside" network, which provides physical and

administrative security to protect the transmission; and a less trustworthy, "outside" network or segment (usually through the Internet). Generally, a firewall sits between a remote user's workstation or client and the host network or server. As the user's client establishes the communication with the firewall, the client may pass authentication data to an authentication service inside the perimeter. A known trusted person, sometimes only when using trusted devices, can be provided with appropriate security privileges to access resources not available to general users.

Types

Secure VPNs use cryptographic tunneling protocols to provide the intended confidentiality (blocking snooping and thus Packet sniffing), sender authentication (blocking identity spoofing), and message integrity (blocking message alteration) to achieve privacy. When properly chosen, implemented, and used, such techniques can provide secure communications over unsecured networks. This has been the usually intended purpose for VPN for some years.

Because such choice, implementation, and use are **not** trivial, there are many insecure VPN schemes available on the market.

Secure VPN technologies may also be used to enhance security as a "security overlay" within dedicated networking infrastructures.

Secure VPN protocols include the following:

- IPsec (IP security) - commonly used over IPv4, and an obligatory part of IPv6.
- SSL/TLS used either for tunneling the entire network stack, as in the OpenVPN project, or for securing what is, essentially, a web proxy. A major practical advantage of an SSL-based VPN is that it can be

accessed from any public wireless access point that allows access to SSL-based e-commerce websites, whereas other VPN protocols may not work from such public access points. OpenVPN, an open standard VPN. Clients and servers are available for all major operating systems.

- PPTP (Point-to-Point Tunneling Protocol), developed jointly by a number of companies, including Microsoft.
- L2TP (Layer 2 Tunneling Protocol), which includes work by both Microsoft and Cisco.
- L2TPv3 (Layer 2 Tunneling Protocol version 3), a new release.
- VPN Quarantine The client machine at the end of a VPN could be a threat and a source of attack; this has no connection with VPN design and is usually left to system administration efforts. There are solutions that provide VPN Quarantine services which run end point checks on the remote client while the client is kept in a quarantine zone until healthy. Microsoft ISA Server 2004/2006 together with VPN-Q 2006 from Winfrasoft or an application called QSS (Quarantine Security Suite) provide this functionality.
- MPVPN (Multi Path Virtual Private Network). MPVPN is a registered trademark owned by Ragula Systems Development Company. See Trademark Applications and Registrations Retrieval (TARR)

Some large ISPs now offer "managed" VPN service for business customers who want the security and convenience of a VPN but prefer not to undertake administering a VPN server themselves.

Trusted VPNs do not use cryptographic tunneling, and instead rely on the security of a single provider's network to protect the traffic. In a

sense, these are an elaboration of traditional network and system administration work.

- Multi-Protocol Label Switching (MPLS) is often used to build trusted VPN.
- L2F (Layer 2 Forwarding), developed by Cisco, can also be used.

Mobile VPNs are VPNs designed for mobile and wireless users. They integrate standards-based authentication and encryption technologies to secure data transmissions to and from devices and to protect networks from unauthorized users. Designed for wireless environments, Mobile VPNs are designed as an access solution for users that are on the move and require secure access to information and applications over a variety of wired and wireless networks. Mobile VPNs allow users to roam seamlessly across IP-based networks and in and out of wireless coverage areas without losing application sessions or dropping the secure VPN session.

However, since VPNs extend the "mother network" by such an extent (almost every employee) and with such ease (no dedicated lines to rent/hire), there are certain security implications that must receive special attention:

- Security on the client side must be tightened and enforced, lest security be lost at any of a multitude of machines and devices. This has been termed Central Client Administration, and Security Policy Enforcement. It is common for a company to require that each employee wishing to use their VPN outside company offices (eg, from home) first install an approved firewall (often hardware).

- The scale of access to the target network may have to be limited.
- Logging policies must be evaluated and in most cases revised.

A single breach or failure can result in the privacy and security of the network being compromised. In situations in which a company or individual has legal obligations to keep information confidential, there may be legal problems, even criminal ones, as a result. Two examples are the HIPAA (the Health Insurance Portability and Accountability Act) regulations in the U.S. with regard to health data, and the more general European Union data privacy regulations which apply to even marketing and billing information and extend to those who share that data elsewhere.

One way to reduce the consequences from a lost or stolen laptop is to use one of the thin client laptops now sold by several companies. These can allow mobile workers to access security-sensitive databases with less risk of lost or compromised data should the laptop be lost or stolen since it has no local storage.

Tunneling

Tunneling is the transmission of data through a public network in such a way that routing nodes in the public network are unaware that the transmission is part of a private network. Tunneling is generally done by encapsulating the private network data and protocol information within the public network protocol data so that the tunneled data is not available to anyone examining the transmitted data frames. Port forwarding is one aspect of tunneling in particular circumstances.

Security dialogues

The most important part of a VPN solution is security. The very nature of VPNs — putting private data on public networks — raises concerns about potential threats to that data and the impact of data loss. A Virtual Private Network must address all types of security threats by providing security services in the areas of:

Authentication (access control) - Authentication is the process of ensuring that a user or system is who the user claims to be. There are many types of authentication mechanisms, but they all use one or more of the following approaches:

- **something you *know*:** a login name, a password, a PIN
- **something you *have*:** a computer readable token (i.e., a Smart card), a card key
- **something *in* you:** fingerprint, retinal pattern, iris pattern, hand configuration, etc

Generally, systems use only of one of these components, usually a login name/password sequence. *Strong* authentication is usually taken to combine at least two authentication components from different areas (i.e., two-factor authentication).

15. Grammar. The Infinitive. See Grammar Reference.

Grammar tasks

Task A. Translate the sentences into Russian. State the function of the infinitive.

We'll consider the formula to be used in our calculations. Computer science is to be regarded as one the most important discipline in technical university. We listened to the professor deliver a lecture. We expect this

profile to be next month. The Arabs were the first to develop the principles of cryptography. To translate this article is difficult. The first step in performing encryption is to locate the two letters from the plaintext into the matrix. The ideas of Protection Profile to be presented were kept secret.

Task B. Find the Infinitive and the Complex Infinitive Constructions. Translate the sentences into Russian.

The only thing for you to do is to use this algorithm. Todygiu is believed to know the problem well. The teacher made the students do the task. The ciphers of this sort are unlikely to be secure. To approach the acceptable level of security, the route should be much more complicated. The order of the columns to be written is determined by the key. This block size is likely to increase to 128 bits. Everybody knows plaintext to be the source of information to be secured.

Task C. Translate into English.

1. Делегация, которую нужно встретить, состоит из студентов и преподавателей.
2. Мы знаем, что первыми, кто использовал шифр, были спартанцы.
3. Л. Б. Альберти известен тем, что он изобрел шифровальный диск.
4. Чтобы читать статьи на английском языке, студенты должны знать термины.
5. Кажется, он не понимает вопросов.
6. Работа, которую нужно завершить, была очень сложной.
7. Для греков простая замена или перестановка букв в посланиях не была чем-то необычным.
8. Целью этого эксперимента было создание новых шифров.

9. Для обнаружения вируса необходимо использовать комплекс программ.

10. Я хочу, чтобы Вы представили свою разработку на конференции.

11. Говорят, что этот вирус заразил каждый пятый компьютер в мире.

12. Этот алгоритм создан для того, чтобы синтезировать речь.

16. Communication. Role play.

Job Interview.

Participants.

Staff Manager.

Candidate 1.

Candidate 2.

Top Manager.

Staff Manager. *You're interested in hiring a young and enthusiastic person. Think of your requirements and questions which will clear out the suitable candidate. Give the comments of your choice.*

Candidate 1. *You've just graduated from … university. You feel quite well-prepared theoretically for the job and have lots of plans. Think and be ready to present your advantages and ideas.*

Candidate 2. *You've got some job experience and good recommendations from your previous job. You're very good at doing practical work. Think of the details and be ready to present your advantages.*

Top Manager. *You have to choose the most suitable candidate. Think of your requirements and questions to the candidates. Be ready to test their knowledge and professional skills and comment on your choice.*

17. Writing. Write your CV. See Appendix 4

Unit 9. FIREWALL

Pronunciation

Make sure you pronounce the following words properly:

distributed [dɪs'trɪbju:t]	determine [dɪ'tə:mɪn]
intermediary [ˌɪntə'mi:djərɪ]	penetrate ['penɪtreɪt]
relevant ['relɪvənt]	flaw [flɔ:]
efficient [ɪ'fɪʃənt]	adequate ['ædɪkwɪt]
unified ['ju:nɪfaɪ]	dual ['dju:əl]

Memorize the terms

1. Read the following terms and their definitions and memorize them:

chart a table of filtering rules – prearrange a set of rules for packet filtering

flag – marker, indicator

information outflow – leakage of confidential information

local firewall – means of protection installed on the computer

outside hub - wiring panel located outside

packet filter – means that processes packets and doesn't allow passing of malicious items

traffic filtering – processing and passing or blocking the information of the internet

2. Match the following words with their Russian equivalents:

software firewall	функциональный уровень
collapsed network	шлюз
distributed firewall	сервер прикладного уровня
functional layer	номер порта отправителя
gateway	рухнувшая сеть
application layer server	программное средство сетевой защиты
source port number	распространяемая система защиты доступа

3. Match the following words with their synonyms:

(packet) proceeding	get, obtain
relevant	let pass
flaw	broken down
gate (v)	movement
gain	intermediary, in-between
collapsed (network)	defect
mediator	significant, meaningful

Reading

4. Pre-reading task.

Do you use firewall? Which one?

Where are firewalls to be used?

What are the principles of their work?

What are the criteria of choosing a firewall?

5. Scan the text and mark the sentences about

- the principles of classification of firewalls;

- the most advantageous method of prevention access to undesirable internet-resources and blocking external attacks;

- how information exchange between driver and application program is realized.

Text 1. Personal firewall.

Problem of information security in global network is very important today because a lot of personal computers have connection to Internet. This problem can be solved by means of using personal firewall. Firewall is a system which allows dividing network by several parts, and realizing a set of rules determining conditions of information between these parts.

Firewalls can be classified by implementation as software, hardware and mixed type; or by component model as local and distributed. But classification by function layer is the most useful. Here we can determine three types of firewalls: packet filters, application layer servers and session layer gateways.

Session layer gateway represents system translating connections outside. User process connects to firewall when access is gaining. Then firewall connects to outside hub. During the work firewall duplicates incoming and outgoing information. Such system is low efficient and doesn’t grant new network services protection.

Application layer server represents mediator between user process and required service. It passes through all traffic and takes a decision about

its safety according to security policy. Such firewall is also low efficient and very expensive.

Packet filtering lies in taking decision of gating or not one or another packet on basis of information about IP-address, source and destination port numbers, flags. Administrator's task involves charting table of filtering rules. This system has high speed of packet proceeding and low cost.

But independently from type firewall must block all known attacks types. Also it must prevent information outflow if harmful code has already penetrated into computer. Control of access to internet-resources is the best way to save labour time of staff.

The most convenient way to prevent access to undesirable internet-resources and to block external attacks lies in packet filtering. Packet filter is configured to filter incoming and outgoing packets on the basis of information containing in TCP and IP headers. This technology is used because rules of filtering can be configured flexible and speed of packet processing is high. Main disadvantage of packet filter is visibility of net configuration from the internet. But this fact is not relevant for personal computer.

There are two methods of traffic filtering. First method lies in developing user application without creating network protocol driver. Such filters are simple in realization, but they don't grant adequate protection.

Another method of traffic filtering adverts directly to core. There are several technologies in this group, but we've chosen TDI-filter. Such personal firewall represents packet filter and consists of driver and application program.

Driver realizes functions of Transport Data Interface (TDI) and intercepts all addresses to original TCP driver to store information about existing connections. Transport Data Interface represents unified program interface for interconnection between transport drivers (TCP driver, for example) and TDI-clients (servers, network interfaces emulators, redirectors). TDI makes TDI-clients independent from used transport protocols.

Application program reflects information about rules and packets and realizes simple user interface. This program receives information about blocked packets from driver. Information exchange between driver and application program is realized by means of standard functions of Win32 Application Programming Interface.

6. Answer the following questions.

What is firewall?

How are the firewalls classified?

Which firewall is considered to be not very efficient and expensive?

Which firewall has most advantages?

Which two methods of traffic filtering are mentioned in the text?

What is Transport Data Interface?

How does application program receive information about blocked packets?

7. Write if the following statements are true or false.

1. Firewalls monitor the information in the Internet and control its passing.

2. The most efficient classification of firewalls is one by implementation.

3. Session layer gateway is the most expensive system of information protection.

4. But session layer gateway is unable to protect new network services.

5. Application layer server is characterized as low effective.

6. The cheapest system is packet filtering.

7. The system of packet filtering operates the information about IP-address, source and destination port numbers, flags in its work.

8. The most serious problem for personal computer is visibility of net configuration from the internet during packet filtering.

9. The main idea of information protection in the Internet is to control of access to internet-resources.

10. TDI-filter intercepts all addresses to original TCP driver and stores information about all connections.

Vocabulary tasks.

8. Give as many word combinations as possible and translate them.

Layer, packet, filter, gate, gateway, application,

9. What do the following abbreviations from Text 1 mean?

IP, TDI, TCP, ICS

10. Make the word combinations.

1. packet	a) firewall
2. filtering	b) proceeding
3. information	c) address
4. traffic	d) configuration
5. session layer	e) hub
6. outside	f) outflow
7. functional	g) gateway

8. distributed	h) rules
9. net	i) filtering
10. IP	j) layer

11. Translate into Russian the following passage.

When a user downloads a virus, worm or Trojan (or it penetrates a gateway security device), intrusion detection systems (IDSs) can issue alerts about those attacks and intrusion prevention systems (IPSs) can block them—if you have enough confidence in the detection signature and if these in-line devices are on the same segment as the security breach. However, these solutions don't effectively address non-signature threats or mitigate a network-wide outbreak.

Furthermore, a greater threat to businesses is posed by non-signature-based malicious or accidental threats such as multiple files sent to an outside e-mail address by an employee preparing to resign or music file sharing that not only uses corporate assets but also opens that employee's entire C: drive. These are much harder to detect and defend against.

12. Complete the text by translating Russian phrases given in brackets.

Like every other component or device in your network, firewalls also (1 необходимо модернизировать) so that they can continue to perform and respond to new threats.

Not that you should be pessimist, but (2 если Вы считаете, что Ваш межсетевой экран устарел еще в тот день, когда Вы его установили), you will be more able to cope with the constant need to

update and cover the new services under your firewall, sometimes, if you have a packet filtering firewall, you may even need to recycle it.

Of course, (3 Вам нужен доступ к Интернет-почте и новостям), vendors, and other users to be a part of the dialog about changes in network security practices. Just as with application upgrades, (4 необходимо добавить новую услугу в Вашу сеть) the day it is issued from the vendors. (5 безопаснее немного подождать и понаблюдать) while the market “shakes out“ the bugs and (6 и будут разработаны новые стратегии безопасности). But without a doubt, (7 Ваш межсетевой экран не вечен), and eventually you will need to recycle it, update it to say the least.

13. Translate into English the following passage.

Для эффективного построения распределенных информационных технологий необходимо участие пользователя в функциях, выполняемых в распределенных устройствах, часто удаленных от места положения самого пользователя. В связи с этим встает задача идентификации и аутентификации пользователей в различных компонентах распределенной системы и программной инфраструктуры в зависимости от выполняемых бизнес-процессов. Существует классификация взаимодействия различных пользователей, которая требует различных решений по идентификации и аутентификации и защите информации в целом. Для служащих компании аутентификация должна позволить обеспечить доступ к различным распределенным приложениям, обеспечивая интеграцию различных приложений и в то же время устанавливая заданные требования по безопасности (B2E).

14. Read the second part of the article and write one sentence to characterize each type of firewall architecture.

Text 2.

On occasion companies choose to implement a firewall based solely on a single machine, be it a router or host. More often than not, however, the stronger firewalls are composed of multiple parts. In this section, we'll take a look at what we consider the five most common types of firewall architectures: the screening router, the dual homed gateway, the screened gateway, the screened subnet, and the "belt-and-suspenders" firewall.

Screening Router

The simplest way to implement a firewall is by placing packet filters on the router itself. This architecture is completely transparent to all parties involved, but leaves us with a single point of failure. Moreover, since routers are primarily designed to route traffic, the default failure mode on routers is usually to pass traffic to another interface. If something were to happen to the router access control mechanism, then the possibility would exist for unauthorized traffic to find its way into the network or for proprietary information to "leak" out of the network.

Moreover, screening routers tend to violate the choke point principle of firewalls. Although all traffic does pass through the router at one point or another, the router merely passes the traffic on to its ultimate destination. Although screening routers can be an important part of a firewall architecture, we don't consider them adequate firewall mechanisms on their own.

Dual-Homed Gateways

Another common architecture places a single machine with two networks as a dual-homed gateway. Such gateway can be used as a generic dual-homed gateway, as described earlier, in which all users must log in to the machine before proceeding on to the other network, or as a host for proxy servers, in which user accounts are not required.

From a "fail-safe" perspective, dual-homed gateways offer a step up from the simple screening router. Nevertheless, dual-homed gateways have certain feasibility and usability problems that don't always make them easy to use.

Screened Host Gateway

Now let's take a look at how hosts and routers can be used together in a firewall architecture. One of the most common combinations in use today is the screened host gateway.

In the screened host gateway scenario, the router is still the first line of defense. All packet filtering and access control is performed at the router. The router permits only that traffic that the policy explicitly identifies, and further restricts incoming connections to the host gateway. This gateway performs a number of functions:

1. It acts as the name server for the entire corporate network.

2. It serves as a "public" information server, offering Web and anonymous FTP access to the world.

3. It serves as a gateway from which external parties can communicate with internal machines.

Screened Subnet

The screened subnet approach takes the idea of a screened host gateway one step further. The screening router is still present as the first

point of entry into the corporate network, and screens incoming traffic between the Internet and the public hosts. Rather than a single gateway, as in the screened host gateway approach, however the functions of that gateway are spread among multiple hosts. One of the hosts could be a Web server, another could serve as the anonymous FTP server, and yet a third as the proxy server host, from which all connections to and from the internal corporate are made.

Functionally, the screened subnet is similar to the screened host gateway: the router protects the gateway from the Internet, and the gateway protects the internal network from the Internet and other public hosts. One distinct advantage that the subnet has over the screened gateway is that it is much easier to implement a screened subnet using "stripped down" hosts, that is, each host on the subnet can be configured to run only those services it is required to server, thus providing an intruder with fewer potential targets on each machine.

Belt and Suspenders Approach

A final architecture takes the idea of the screened subnet and extends still another step further. The principles are the same as the subnet architecture: an external screening router protects "public" machines from the Internet. Instead of a gateway running proxy server software as well as protecting the internal network, however, those functions are split: the proxy server host now resides on the DMZ subnet, while an internal screening router serves to protect the internal network from the public machines. This architecture is often called the "belt-and-suspenders" architecture.

The belt-and-suspenders architecture is only subtly different from the screened subnet, but the difference is important from a security point of view. Whereas the subnet relies on the proxy servers to perform all access control to and from the internal network, the belt-and-suspenders approach relies on the proxy server as the first line of authentication defense, but the internal router serves to back up the server, as well as to protect the internal network from the machines on the public network.

15. Grammar. The Participle. See Grammar Reference.

Grammar tasks

Task A. Translate the sentences into Russian. State the function of the participle.

The unpolarized photons are blocked by polarization filters. While testing the equipment you should put down the results. Having been discovered many years ago, this method was put to practical use only last year. When included, the elements of the risk assessment project help to avoid confusion and misunderstanding. The fuzzy matching of biometrics cannot be performed in the encrypted domain. The security of this method is dependent on the security of the key being hidden and retrieval algorithms. The described biometrics-based keys allow both performing user authentication by biometric component and handling secure communications by a generic cryptographic system.

Task B. Find the Participle and the Complex Participial Constructions. Translate the sentences into Russian.

Sometimes a user doesn't want engineered authentication systems to be used. Data can be recovered from cipher only by using exactly the same key used to encipher it. When implemented in accordance with FIPS 140-1

other FIPS approved cryptographic algorithms may be used in addition to this standard. When correctly implemented and properly used, this standard will provide a high level of cryptographic protection to computer data. The protection provided, this algorithm will be reviewed within 5 years to assess its adequacy. The cryptographic algorithm specified in this standard transforms a 64-bit binary value in to a unique 64-bit binary value based on a 56-bit variable. Authentication being done the biometrics matching would be carried out in the transformed space. The scientist working at this problem is well-known.

Task C. Translate into English.

1. Мы не видели, как наш коллега готовился к выступлению.
2. Описанный метод имеет ряд недостатков.
3. Это самый надежный из известных способов защиты информации.
4. Когда я готовился к конференции, мне пришлось просмотреть все мои записи.
5. Когда моему отцу предложили работу за границей, он отказался уезжать из своей страны.
6. После того как контракт был подписан, мы отправились домой.
7. Я хотел бы, чтобы эта статья была написана Вами.
8. После того как межсетевой экран был установлен, атаки извне стали блокироваться.
9. При выборе криптографического протокола обратите свое внимание на наиболее часто используемые.
10. Будучи широко распространенными, многоразовые пароли способствуют нарушению безопасности.

16. Communication

Project work. Imagine that you are a senior manager responsible for Intranet security of an enterprise. Work out a set of corporate rules aimed at information protection. Think of all possible risks and security solutions. Make a presentation and be ready to discuss the problem you're going to solve in your project.

17. Writing.

Write an abstract of your project.

Unit 10. WIRELESS COMMUNICATION

Pronunciation

Make sure you pronounce the following words properly:

overlap (n) ['əuvəlæp]	circuit ['sə:kɪt]
overlap (v) [əuvə'læp]	issue ['ɪʃu:]
nomadic [nəu'mædɪk]	knot [nɔt]
scheme [ski:m]	malicious [mə'lɪʃəs]

Memorize the terms.

1. Read the following terms and their definitions and memorize them:

security compromise – security failure, breech of protection system

assets of an enterprise – amount of property, tangible and intangible like stocks, physical capital, buildings, equipment, documents, developments and all information connected with the work of an enterprise

two-way radio – receiver-transmitter, send-receive set

PDA – Personal Digital Assistant, electronic device used as electronic organizer/secretary

data rate – rate of information exchange

inbound traffic – incoming information

2. Match the following words with their Russian equivalents:

bandwidth	специальная телесеть
low power consumption	непостоянный, временный доступ
two-way radio	статистически назначенный адрес
ad hoc network	полоса пропускания
nomadic access	обработка данных на коммутаторе каналов
statically-assigned IP address	приемно-передающая радиоустановка
circuit switched data service	малое энергопотребление

3. Match the following words with their synonyms:

node	match (partially)
(data) rate	agreement
cordless (system)	penetrator, attacker
overlap	knot
inbound	speed
intruder	deceive
compromise	incoming
spoof	battery-operated

Reading

4. Pre-reading task.

Which wireless devices can you name?

Which ones are most commonly used?

What can you say about Wi-Fi protection means?

What are the perspectives of their development?

5. Text 1. Read the text and outline the main problems of wireless communication security and the perspectives of protection means.

An overview of the security of wireless networks.

More and more applications are being accessed through wireless systems, including commerce, medical, manufacturing, and others. Wireless devices have become an extension of corporate databases and individuals. Their security compromises are as serious as any attack to the corporate database and may have damaging effects on the privacy of individuals and the protection of assets of an enterprise. Wireless devices include cellular phones, two-way radios, PDAs, laptop computers, and similar. These are normally portable devices with limitations of weight, size, memory, and power. The increase in functions in cellular devices creates new possibilities for attacks. Standard attacks against the Internet may now take new forms. Lists of vulnerabilities are already available, showing flaws in many existing products.

Communicating in the wireless environment has its own issues and challenges. It is characterized by relatively low bandwidth and data rates, as well as higher error rates, and the need for low power consumption (for mobile devices). The mobility of the nodes in cases such as ad hoc networks adds another significant layer of complexity and unpredictability.

There exist many different forms of wireless communications and networking.

Some popular forms of wireless communications include:

Satellite communication;

Cellular networks, Cordless systems;

Mobile Internet Protocol (Mobile IP);

Wireless Local Area Networks (WLANs) including LAN extensions, Cross-building interconnects, Nomadic access, Mobile ad hoc networks (MANETs).

The security of wireless systems can be divided into four sections:

1. Security of the application. This means the security of user applications and standard applications such as email.

2. Security of the devices. How to protect the physical device in case it is lost or stolen.

3. Security of the wireless communication. How to protect messages in transit.

4. Security of the server that connects to the Internet or other wired network. After this server the information goes to a network with the usual security problems of a wired network (not discussed here).

There is serious concern about the vulnerabilities of wireless systems. The easy access to the medium by attackers is a negative aspect compounded by the design errors in the early protocols. The US Department of Defense recently issued Directive 8100.2 that requires encrypting all information sent in their networks according to the rules of the Federal Information Processing (FIP) standard. The provision also calls for antivirus software.

On the other side, Ashley et al. arrived to the conclusion that WAP provides excellent security. It is true that Wi-Fi is becoming more secure and Bluetooth appears reasonably secure but they (and WAP) cover only some of the security layers. A basic security principle indicates that security is an all- layer problem, one or more secure layers is not enough.

Third generation systems will have voice quality that is comparable to public switched telephone networks. Voice over IP will bring its own set of security problems. The new systems will have also higher data rates, symmetrical and asymmetrical data transmission rates, support for both packet and circuit switched data services, adaptive interface to the Internet to reflect common asymmetry between inbound and outbound traffic, more efficient use of available spectrum, support for wide variety of mobile equipment, and more flexibility. All of these are the potential sources of new security problems.

Web services are not delivered directly to portable devices but transformed in the gateway. However, this situation is changing and predictions indicate that web services in cell phones will be arriving soon.

Security patterns are a promising area to help designers build secure systems. Several patterns have been found in the Bluetooth architecture, including versions of the Broker, Layers, Lookup, and Bridge patterns. However, no security patterns for wireless systems have been found yet. This is an area to explore.

6. Answer the following questions.

What are the peculiarities of wireless communication?

What are the forms of wireless communication?

How can the security of wireless systems be classified?

What are the contradictory opinions of experts about wireless security?
What is the forecast of wireless systems protection?

7. Mark the following statements "true" or "false". Correct the false statements.

1. An access to corporate and private data is often gained via wireless devices now.
2. Security breeches in wireless devices don't have as disastrous outcomes as in corporate networks.
3. Modern information protection systems aren't efficient in counteracting the attacks against wireless devices.
4. Nomadic access implies permanent access.
5. Security of the application protects using e-mail.
6. Security of the wireless communication helps to protect the process of sending and receiving messages.
7. The vulnerability of wireless systems is still underestimated.
8. Bluetooth is considered to be the most secure.
9. Further development of third generation systems will lead to new information protection problems.

Vocabulary tasks

8. What do the following abbreviations from Text 1 mean?

PDA, WLAN, IP, MANET

9. Give your definitions of the following terms.

wireless environment, vulnerability, smart device, security pattern, flaw, assets of an enterprise

10. Make the word combinations.

1. data	a) network
2. nomadic	b) compromise
3. inbound	c) rate
4. two-way	d) interconnect
5. cordless	e) of an enterprise
6. power	f) traffic
7. ad hoc	g) access
8. cross-building	h) radio
9. security	i) system
10. assets	j) consumption

11. Translate into Russian the following passage.

In recent years, many authentication protocols for the wireless network have been proposed. When a mobile user is roaming in wireless environment, it is desirable to protect the relevant information about him. Assuring the anonymity of a mobile user prevents unintended parties from associating him with the messages to/from him or with the sessions in which he participates. The disclosure of a mobile user's identity allows unauthorized entities to track his moving history and current location. The illegal access to any information related to users location without his notice can be a serious violation of his privacy. So, anonymity is one of importance property of these protocols.

A basic solution for the provision of user anonymity is to use the temporary identity (TID) of a mobile user instead of his real one. Our proposed authentication scheme is based on the public key cryptosystems, but mobile users only do symmetric encryption and decryption.

12. Translate into English the following passage.

Регулярные исследования в области беспроводных сетей и протоколов помогают нам получить представление о реальном положении дел в этой области. Мы стараемся освещать эти вопросы в наших статьях, чтобы привлечь к ним внимание пользователей. Основными объектами нашего исследования являются Wi-Fi точки доступа и мобильные устройства с поддержкой протокола Bluetooth.

Мы планировали собрать статистику по Bluetooth-устройствам на выставке, в парижском метро и просто на улицах города. До сих пор нам ни разу не удавалось зафиксировать наличие хотя бы одного из мобильных червей — Cabir или Comwar — в крупных городах мира, но на Францию мы возлагали особые «надежды», связанные с тем, что первый мобильный червь (Cabir) был создан именно там.

14. Text 2. Read the text and write down the main ideas of its parts.

1	
2	
3	

1. Gateways are devices that control the flow of traffic into or out of a network. Although definitions differ, for this context a gateway can be thought of as a device that passes packets between subnets (real or virtual), and performs operations above OSI layer 3 (session, flow control, protocol conversion, and application specific). Gateways can also be the source of vulnerabilities. Gateways are important to wireless networks and mobile wireless devices for several reasons:

Wireless networks do not afford the same physical levels of security as wired networks. Due to resource constraints, mobile wireless devices are themselves often less secure than wired devices. *Wireless security gateways* can protect a wired network from untrusted wireless hosts. Unlike firewalls, for which hosts are either "inside the firewall" or "outside the firewall," the distinction between inside and outside is somewhat blurred for mobile wireless devices. A company's trusted workers may need "inside" kinds of connectivity while using wireless devices. Conversely, visitors may need "outside" kinds of connectivity while connecting to the company's wired network through an access point inside the corporate firewall. Wireless security gateways address these issues by performing two-way authentication and limiting access privileges on a per-device basis.

2. Mobile wireless devices often have limited resources that cannot support the same protocols as wired devices. They may therefore use resource-sharing protocols which must be translated in a protocol gateway to enable interaction with standard Internet protocol services. For example, a *WAP gateway* translates protocols in the WAP suite, including WML (HTML), WML Script (CGI), WBMP (BMP), WBXML (XML), WSP (HTTP), WTP (TCP/IP), WTLS (SSL), and WDP (UDP).

These kinds of translation pose security issues both because the wireless protocols are often less secure than the corresponding wired protocols, and because, in translation, encrypted data takes an unencrypted form inside the gateway.

Wireless devices often exist on subnets that do not support the full Internet addressing scheme. For example devices may use IP addresses

reserved for local access only, or otherwise not support all of the capabilities needed for WAN access. Gateways can provide a bridge between these local subnets and a broader WAN, (i.e., Internet). Common SOHO wireless switches provide NAT to allow local devices to all access the Internet using a single IP address. Similarly, a Personal Mobile Gateway with WAN connectivity like GSM/GPRS can allow Bluetooth, 802.11, or 802.15 devices on a PAN to have full Internet connectivity.

The fact that devices behind a NAT gateway do not have unique IP addresses has implications for some security strategies (i.e., IPSEC-AH).

Mobile wireless devices may be involved in various sorts of commerce, such as M-commerce and downloading multimedia streams with digital rights.

Depending on how you look at it, where conflicting privacy and ownership interests come into play, “trusted gateways” can bridge the no man’s land, or encapsulate the overlap as a trusted third party. This space is an area of active research and is, as yet, not as well defined as the other gateway functions. Issues here are closely tied to digital rights management. See for example the Shibboleth project.

The Internet was built on “transparency” and the “end-to-end principle”. Roughly stated, transparency “refers to the original Internet concept of a single universal logical addressing scheme, and the mechanisms by which packets may flow from source to destination essentially unaltered.” The end-to-end principle holds that functions of data transmission other than transport, such as data integrity and security, are best left to the transmission endpoints, themselves. This allows applications to be ignorant of the transport mechanisms, and transport

systems to be ignorant of the data being transported. Gateways, by their nature, violate one or both of these principles.

3. *Gateway deployment strategies*

At the basic network level, gateways are viewed as servers or end-systems. But gateways create their own overlay networks and may be involved in ISO level 2 and level 3 routing. The use of gateways can greatly complicate problems of network management. Their deployment should be carefully considered within a comprehensive network coverage and security strategy.

The main reason for using a wireless security gateway is that intruders may gain access through an insecure wireless access point and mount an attack on the internal network.

802.11b, Bluetooth, and WAP are all potentially insecure. Access points with stronger security are possible using Cisco or 802.1x protocols. Typically, a large site or campus, will need many access points for good coverage. The cost of numerous high-end access points and the problem of managing them, especially when they are not all from the same vendor, is a major concern. A common strategy is to use simple (“thin”) access points and put one or more security gateways between all wireless access points and the wired network. Then even if anyone can establish a connection to an access point, they will be challenged at the gateway. The gateway might use IPSEC, VPN, and/or LDAP encryption and authentication.

Several strategies are available to ensure that access points connect only to a gateway.

Access points could be physically wired on a separate subnet where gateways provide the only bridge to the main wired network. Over a large area, the need to maintain two wired networks, one for access points, may be impractical. Multiple smaller networks can be used, each with its own gateway. Multiple gateways can share a common, central management tool – like CA or HP OpenView. They may also be arranged in master/slave relationships, i.e., for configuration and fail-over. Another alternative is to use access points that VPN tunnel to a single gateway, using the regular wired network as the transport medium.

Gateways can grant different users different levels of trust. The easiest way to set this up is to differentiate users by their IP address, and grant different levels of service (i.e., bandwidth) and different kinds of access (i.e., specific protocols like ftp and http, and specific destination hosts) using ISO level 2 (IP address) and level 3 (protocol type) filtering. Access classes can be grouped by role, and identified by predefined ranges of IP address.

15. Sum up the ideas of the text orally.

Vocabulary and Grammar 7-10. Revision.

I. Write if the sentences are true or false. Correct the false sentences.

1. The access of organization to the global network INTERNET essentially increases its functioning effectiveness as well as vulnerability of its assets.
2. Level 4 is the lowest level of authentication assurance.

3. Trusted VPNs use cryptographic tunneling, and don’t rely on the security of a single provider's network to protect the traffic.

4. According to the classification by function layer we can determine two types of firewalls: packet filters and session layer gateways.

5. The easy access to the medium by attackers in wireless communication is a negative aspect compounded by the design errors in the early protocols.

6. To solve the problem of information protection in the Internet it’s necessary to involve legislative measures of protection.

7. Most security breaches in Intranet are committed by clients.

8. Corporate databases include wireless devices.

9. Extranets allow customers and business partners’ access to the intranet.

10. Firewalls can be classified by component model as software, hardware.

II. Complete the sentences using the words given below.

Visibility, portable, threats, identical, firewalls, portable, securing, evaluate, outgoing, reveal.

1. The traditional cryptosystems (e.g., symmetric ciphers as AES and asymmetric ciphers such as RSA) are designed to accept only _____ keys used for encryption and decryption.

2. The software protecting tools are program complexes intended to _____ and to prevent the possible UAA threats.

3. Businesses must _____ their risk level before implementing a security policy.

4. Main disadvantage of packet filter is _____ of net configuration from the internet.

5. Wireless devices are normally _____ devices with limitations of weight, size, memory, and power.

6. Every information protecting mean is directed to the certain type of safety _____.

7. Another key technology for _____ intranets is encryption.

8. Packet filter is configured to filter incoming and _____ packets on the basis of information containing in TCP and IP headers.

9. Wireless devices are normally _____ devices with limitations of weight, size, memory, and power.

10. Perhaps the most well-known measure for securing intranets is the use of _____.

III. Match the lines.

1. unauthorized	a) outflow
2. reusable	b) signature
3. security	c) access
4. internal	d) traffic
5. data	e) password
6. outside	f) breach
7. information	g) user
8. outbound	h) hub
9. nomadic	i) theft
10. digital	j) risk

IV. Choose the correct form of the verb.

1. In this article, we *were examined / have examined / have been examined* several Internet-centric firewall designs in an attempt to meet security and performance requirements of multitier applications.

2. When designing a network, consider how other components of its perimeter (intrusion detection systems, routers, and VPNs) *may / should / must* influence the security of infrastructure.

3. In this design, all servers *host / are hosted / are hosting* on the same subnet, and *warrant / are warranted / are warranting* equal protection by the firewall that *separate / separates / is separated* them from the Internet.

4. Many approaches *explored / have explored / have been explored*, but choices about how to optimize the elliptic curve group operation often *depend / are depend / are depended* on the relative costs of operations.

5. Worms are programs that *can / should / have to* run independently and travel from machine to machine across network connections; worms *can / should / have to* have portions of themselves running on many different machines.

6. A true virus is a sequence of code that *inserts / is inserting / is inserted* into other executable code, so that when the regular program *runs / is running / is run*, the viral code *executes / is executing / is executed*.

7. There *is/has been/is been* very little progress in the solution of this problem since then.

8. Cryptographers *interest/are interesting/are interested* in two main classes of problems.

9. The security of the RSA algorithm *depends/is depending/is depended* on the factoring problem.

10. Cyberterrorists *use/are using/are used* computers, electronic networks and IT for achievement of the terrorist purpose.

V. Put the verbs in brackets in the correct form. There are some non-finite forms necessary.

1. Speech synthesis (base) on MBROLA algorithm (produce) high quality speech.
2. This method (propose) by the authors (detect) complex attacks.
3. The fingerprint image (need) a resolution of 500 dpi.
4. Quantum Key Exchange (also/know) as Quantum Key Distribution.
5. Such systems (call) hybrid systems.
6. The authentication mechanism (use) (provide) the authentic channel may or may not be secure.
7. Systems (use) Quantum Key Exchange require a quantum channel between the communication parties.
8. Bacteria, also known as rabbits, are programs that (not damage) any files explicitly.
9. The goal of our experiment was (evaluate) empirically the number of distinguishing features for the average user.
10. (Eliminate) reliance on a single firewall you can use multiple firewalls to guard subnet boundaries.

VI. Give definitions of the following terms.

Security outsourcing, embedding of a program, chart a table of filtering rules, repository, internal risk, proactive, intrusion, integrity, misconception, software firewall.

VII. Translate into Russian.

Security management systems protect employees, buildings, office equipment, stock and intellectual property. ISGUS hardware and software applications are an effective solution to diverse security requirements at all time.

Organizational structures and employee tasks change over time and therefore security areas, room zones and authorizations for staff and visitors must be flexible and facilitate fast and efficient administration.

VIII. Translate into English.

Несмотря на опасность перехвата конфиденциальной информации, хищения личных данных и нарушения нормального функционирования мобильных устройств, только единицы пользователей обеспокоены проблемой защиты. Подавляющее большинство абонентов не уделяет вопросам безопасности должного внимания, не считая эти угрозы критичными.

Между тем от действий злоумышленников могут пострадать и абоненты сетей сотовой связи, и операторы, и производители. Чтобы свести к минимуму возможные потери от инцидентов и противостоять новым угрозам, игрокам рынка и абонентам необходимо уже сейчас принимать упреждающие меры.

IX. Translate into English using non-finite forms of the verbs.

1. Этот метод, открытый много лет назад, стал использоваться лишь недавно.

2. После того, как был проведен анализ рисков, руководству был предложен ряд мер по защите информационных активов.

3. Мы знаем, что первые шифровальные машины были изобретены в Древней Греции.

4. Выполнить это задание - нелегко.

5. Первое руководство по криптографии в Европе, включающее различные виды шифров, было создано в Италии.

6. Будучи хорошо продуманной, система безопасности предприятия не допускала нарушений.

7. Разработанный межсетевой экран имеет ряд преимуществ.

8. Вероятно, разработка надежных средств аутентификации – нелегкая задача.

9. Разработка, основанная на этом методе, представлена в докладе.

10. После обнаружения вирус уничтожается.

X. Communication

Project Presentation

Chairman. *Study the project beforehand. Be ready to conduct the meeting, ask your questions and make some conclusions.*

Developers. *Present your project. Try to point out the advantages of using your development.*

Consumers. *You're interested in buying the product which will be efficient and cost-effective. Think of your questions to the developers and comment on your choice.*

Secretary. *Be ready to make notes of the presentation, questions and answers.*

XI. Writing. Write the abstract of your project work.

APPENDIX 1

GRAMMAR REFERENCE

Unit 3

Passive Voice

<table>
<tr><td></td><td colspan="4">Passive</td></tr>
<tr><td></td><td>Simple</td><td>Progressive</td><td>Perfect</td><td>Perfect Progressive</td></tr>
<tr><td>Present</td><td>sometimes, every day, often, always, etc.
am
is asked
are</td><td>now, still, at the moment
am
is being asked
are</td><td>already, ever, just, never, yet
have
been asked
has</td><td rowspan="5">Вместо отсутствующих форм Perfect Progressive употребляются формы Perfect</td></tr>
<tr><td>Past</td><td>yesterday, two years ago, in 1995, etc.
was
asked
were</td><td>when he came, at that moment, etc.
was
being asked
were</td><td>by the time, already, etc.
have
been asked
has</td></tr>
<tr><td>Future</td><td>tomorrow
will be asked</td><td>вместо отсутствующей формы Future Progressive употребляется Future Simple</td><td>by the time in the future
will have been asked</td></tr>
<tr><td>Инфи-нитив</td><td>be V₃</td><td>be being V₃</td><td>have been V₃</td></tr>
</table>

Unit 5

Modal Verbs

Употребление.

Выражение способности или умения что-либо делать.

Can- мочь, уметь, **be able to-** быть в состоянии.

Выражение возможности (вероятности).

May - определенная степень вероятности,

Might - большая степень вероятности. They may be at work. There might be some sugar in the cupboard**.**

Must – уверенность. They look alike. They must be twins.

Can't – кажется невозможным. You've been sleeping all day. You can't be tired.

Can … be – возможно ли**.** Can she still be at school?

Выражение разрешения в вопросах.

Can – неформальное. Can I borrow your pen?

Could – более вежливое. Could I borrow your car?

May – формальное. May I use your phone?

Might – еще более формальное. Might I see your driving license please?

Выражение разрешения в ответах.

Can – неформальное разрешение. You can have my pen.

May – формальное разрешение. You may come in.

Mustn't, can't – запрет. You mustn't park here. You can't enter this room.

Выражение предложения.

Would you like, shall I/ shall we – вежливое предложение.

Would you like some coffee please? Shall we buy him a present?

Выражение просьбы.

Can – просьба. Can you help me finish my work?

Could – вежливая просьба). Could I have some more paper?

Will – неформальная просьба. Will you help me?

Выражение совета.

Should/ought to, had better.

You should walk more. You'd better rewrite this passage.

Выражение долженствования (необходимости).

Must – обязанность. We must obey the laws.

Have to - необходимость, продиктованная внешними факторами. I have to be at work at 8.30.

I've got to – неформальное выражение личной необходимости. I've got to leave.

Needn't, don't have to – отсутствие необходимости.

Выражение запрета.

Mustn't, can't – запрет. You mustn't park here. You can't enter this room. It's room for the staff.

Unit 7.

The Gerund.

Употребление. Герундий – неличная форма глагола, имеющая признаки как существительного, так и глагола и выражающая действие, как процесс. Самостоятельно вне контекста на русский язык не переводится, так как в русском языке аналогичных форм нет. Герундий, в зависимости от его функции в предложении, переводится отглагольным существительным, инфинитивом, деепричастием или целым предложением (чаще придаточным). Обороты с герундием широко используются в научно-технической литературе.

Образование. Герундий образуется путем прибавления окончания – **ing** к основе глагола и выражает отвлеченное понятие о действии, не указывая на число, лицо и наклонение.

Герундий в функции подлежащего может переводиться существительным или инфинитивом.

Using virtual environments has considerably widened the range of training possibilities. Использование виртуальной реальности существенно расширило возможности обучения.

Measuring temperatures is necessary in many experiments. Измерять температуру

необходимо при многих опытах.

Именная часть составного именного сказуемого переводится существительным или инфинитивом.

One more fact is worth mentioning. Стоит упомянуть ещё один факт.

I can't help being surprised at their success. - Не могу не удивляться их успеху.

Герундий в функции дополнения переводится существительным, придаточным предложением, инфинитивом.

Most memory training systems involve associating the things you want to remember with something you already have safely stored in your head. Большинство систем, тренирующих память, включают процесс ассоциирования вещей, которые вы хотите запомнить, с чем-то, что вы уже надежно запомнили.

Герундий в функции дополнения употребляется:

– после глаголов, выражающих предпочтение **like, love, hate, enjoy, prefer** и других и после глаголов, выражающих начало, конец и продолжение действия **start, begin, continue, finish** и других. Нужно иметь в виду, что после них может употребляться и инфинитив, без особого изменения значения высказывания;

– после глаголов **stop, regret, remember, forget, mean, go on** может употребляться и герундий, и инфинитив, но значение высказывания при этом меняется, что, соответственно отразится и на переводе.

Герундий в функции предложного дополнения переводится существительным или придаточным предложением.

There are many stories about dolphins saving sailors from drowning. Существует много историй о том, как дельфины спасали тонущих моряков от гибели.

The present project aims at promoting an active role of the astronomers. Данный проект нацелен на формирование активной роли астрономов.

Всегда употребляется герундий после следующих глаголов: to be capable of, to depend on, to consist in, to result in, to be interested in, to feel like, to look like, to prevent from, to accuse of, to reply on, to approve of, to insist on, to agree to, to be tired of, to think of, to complain of, to rely on, to speak of, to suspect of, to look

forward. It looks like raining. Похоже на дождь. They insisted on prolonging the negotiations.

В функции определения герундий обычно употребляется с предлогами "of", "for", "in"**.** Переводится существительным с предлогом или неопределенной формой глагола, а также существительным в родительном падеже.

The difficulties in designing these devices led to the development of a new technological method. Трудности в разработке данных приборов привели к развитию нового технологического метода.

Герундий в функции обстоятельства употребляется с предлогами и переводится существительным с соответствующим предлогом или деепричастием.

A system can be realized by making a superconducting tunnel junction. Можно реализовать систему, обеспечив сверхпроводящее туннельное соединение.

On being heated to a sufficient temperature any body becomes a source of light. Любое тело, нагретое до нужной температуры, становится источником света.

The Complex Gerundial Constructions.

Употребление. Сочетание герундия с предшествующим ему притяжательным местоимением или существительным в притяжательном или общем падеже называется **сложным герундиальным оборотом.** Такой оборот обычно переводится придаточным предложением, с вводными словами «то, что», «того, что», «о том, что».

Существительное или местоимение, стоящее перед герундием, становится в русском языке подлежащим придаточного предложения, а герундий – сказуемым.

The man's coming so early surprised us. То, что этот человек пришел так рано, нас удивило.

I never doubted his working in this field of science. Я никогда не сомневался в том, что он работает в этой области науки.

We looked forward to the contract being signed. Мы с нетерпением ожидали

подписания контракта.

Unit 8

Инфинитив с частицей – to.

Употребление. Инфинитив – это основная форма глагола. Его формальным показателем является частица – **to**. Инфинитив имеет следующие формы**.**

Forms	**Active voice**	**Passive voice**
Simple	to translate	to be translated
Continuous	to be translating	–
Perfect	to have translated	to have been translated
Perfect Continuous	to have been translating	–

Simple Infinitive – обозначает действие, одновременное действию, выраженному глаголом-сказуемым. I am glad to see you. Рад тебя видеть.

Continuous Infinitive – обозначает действие, которое развивается одновременно с действием, выраженным глаголом - сказуемым. It is pleasant to be walking along the shady alley. Приятно идти по тенистой аллее.

Perfect Infinitive обозначает действие, которое предшествовало действию, выраженному глаголом-сказуемым. I am sorry not to have helped you. Мне жаль, что не смог тебе помочь.

Perfect Continuous Infinitive – обозначает действие, которое длилось в течение определенного периода времени до настоящего момента. It seems to have been raining since the very morning. Кажется, дождь идет с самого утра.

Passive Infinitive – инфинитив переходных глаголов имеет две формы пассивного залога (Simple and Perfect). В отрицательных предложениях перед инфинитивом ставится – **not.** We decided not to go out because of the weather. Мы решили не гулять из-за погоды.

Инфинитив без частицы – to.

Употребление. Используется в следующих случаях.

После вспомогательных глаголов. I don't understand.

После модальных глаголов. If one cannot have what one loves, one must love what one has.

После глаголов чувственного восприятия. I never saw you look so well before. Я никогда не видел Вас таким раньше.

После глагола to let. **После глагола to make (заставлять).**

После конструкций had better, would rather, would sooner.

***Функции инфинитива в предложении*.** В простейших случаях английский инфинитив не отличается от русского.

Если инфинитив стоит в начале предложения, а за ним стоит сказуемое, то он выполняет функцию **подлежащего** и переводится на русский язык инфинитивом или существительным. To read is useful. Читать - полезно.

Инфинитив выполняет функцию части составного именного сказуемого, если стоит после глагола **to be.** The purpose of this test is to determine the mechanical characteristics of the material. Цель испытания – определить механические характеристики материала.

Инфинитив, стоящий после сказуемого или косвенного дополнения, выступает в функции **прямого дополнения.** I like to read. Я люблю читать.

Основные особенности, отличающие английский инфинитив от русского.

Инфинитив, стоящий в начале предложения до группы подлежащего или **после сказуемого**, выполняет функцию **обстоятельства цели** и переводится на русский язык придаточным предложением с союзами «чтобы», «для того, чтобы». Laws were not made to be broken. Законы созданы не для того, чтобы их нарушать.

Инфинитив цели может вводиться словами in order to, so as.

Инфинитив в роли определения, стоящего после определяемого слова, чаще бывает в форме пассивного залога и переводится на русский язык придаточным определительным предложением с оттенком будущности и модальности. The strength of radio waves to be measured is expressed in microvolts. Сила радиоволн, которая должна быть измерена, выражается в микровольтах.

The Infinitive Constructions.

В научной литературе встречаются также инфинитивные обороты двух типов.

Complex Object.

Употребление. **Сложное дополнение** используется в научной литературе для соединения двух простых предложений, например, по формуле: Smb. did smth. + I saw this = I saw smb. do smth.

I saw him cross the street. Я видел, как он переходил улицу.

The scientist consider the sun to emit radio signals. Ученые считают, что солнце испускает радиосигналы.

В таких оборотах используются глаголы: **see, hear, feel, notice, smell, find, know, think.** На русский язык придаточное предложение переводится с помощью союзов «как, что». После глаголов **want, wish** при переводе придаточное предложение начинается с союза «чтобы»: I want him to open the door. Я хочу чтобы он открыл дверь.

Complex Subject.

Употребление. **Сложное подлежащее** состоит из подлежащего, выраженного существительным в общем падеже или местоимением в именительном падеже и инфинитива. Между компонентами оборота стоит сказуемое, которое может быть выражено следующими четырьмя способами.

Глаголом в форме страдательного залога, например, is said, is known, is supposed, is believed, is assumed, is thought, is considered, is found.

These tubes are said to give considerable economy. Говорят, что эти лампы дают значительную экономию.

Глаголами в форме активного залога, например, to seem, to appear, to prove, to happen. Перевод начинается с вводного слова «кажется, оказывается». He seems to know English. Кажется, он знает английский.

Инфинитив употребляется со словосочетаниями to be likely, to be unlikely, to be certain, to be sure. He is likely to know English. Вероятно, он знает английский.

Инфинитив с for. It is not unusual for restored cars to sell for more than they did when new. Для реставрированных машин не является необычным тот факт, что они продаются дороже, чем стоили, когда были новыми.

Unit 9

Причастие - это неличная форма глагола, которая обладает признаками **глагола, прилагательного и наречия.** В современном английском языке имеются два причастия: причастие I (Participle I) и причастие II (Participle II).

Participle I (Simple, Perfect) образуются при помощи инфинитива без частицы "to" с прибавлением суффикса – **ing.**

Participle II образуются путем прибавления к основе глагола суффикса - ed (правильные глаголы, e.g. look+ed). **Participle II** неправильных глаголов является их третьей формой, что видно в таблице неправильных глаголов, например, gone, spoken, taken и другие. **Participle II** имеет только форму страдательного залога.

Participle I.

Употребление. Причастие I активного залога (Participle I, Simple, Active) может выполнять в предложении функции **определения и обстоятельства**.

В функции определения Participle I, Active может стоять перед определяемым словом (левое определение). Переводится на русский язык **причастием настоящего времени** с суффиксами –ущ-, -ющ-, -ащ-, -ящ- или причастием прошедшего времени с окончанием - вший. They looked at the flying plane - Они смотрели на летящий (летевший) самолет.

Если причастие I стоит после определяемого слова (правое определение), то на русский язык оно переводится **причастным оборотом или определительным придаточным предложением.** A magnet attracts only objects containing iron. Магнит притягивает только предметы, содержащие железо.

Причастие I страдательного залога (Participle I, Passive) на русский язык переводится **причастием страдательного или действительного залога** с окончаниями -мый, -щийся или **определительным придаточным предложением.** The bridge being built across the river is very beautiful. Мост, строящийся через реку (который строится через реку), очень красивый.

В функции определения причастие I (Participle I, Simple, Active or Passive) может стоять в начале предложения (иногда с союзами **when, while)** или в конце предложения. Переводится следующими тремя способами.

1. **Деепричастием**, оканчивающимся на -а(сь), -я(сь). He spent the whole day preparing for his exams. Он провел весь день, готовясь к экзаменам.

2. **Обстоятельственным придаточным предложением**. Being repaired recently the bridge was in good condition. Будучи недавно отремонтированным, мост был в хорошем состоянии (Так как мост недавно отремонтировали, он был в хорошем состоянии).

3. **Существительным с предлогом "при".** When translating a scientific article he met a lot of difficulties. Переводя статью (при переводе, когда переводил статью) он встретился со многими трудностями.

Participle I, Perfect, Active (having analyzed) может переводиться на русский язык **деепричастием совершенного вида**, оканчивающимся на -ав или придаточным предложением.

Having analyzed the properties of the substance they made some new conclusions. Проанализировав свойства вещества, они сделали новые выводы.

Participle I, Perfect, Passive (having been given) переводится, как правило, **придаточным предложением**. Having been given all the instructions he began his work. После того как он получил все указания, он начал работать.

Participle II.

Употребление.

Если причастие II является левым определением, то на русский язык оно переводится **причастием страдательного** залога с оканчивающимся на -ный, -тый, -мый. The described method is widely used in industry. Описанный метод широко используется в промышленности.

Если причастие II является правым определением, то на русский язык оно переводится **причастным оборотом** или **определительным придаточным предложением.** The equipment tested requires further

improvement. - Испытываемое оборудование требует дальнейшего усовершенствования.

Если причастие II употребляется в функции обстоятельства, то оно может стоять в начале предложения (перед подлежащим) и в конце предложения. Перед **Participle II** могут употребляться союзы if (если), unless (если не), while (в то время как), when, as и другие. В этом случае на русский язык причастие переводится тремя способами.

1. **Обстоятельственным придаточным предложением**. If heated, molecules of the material move faster. Если молекулы вещества нагреть, они движутся быстрее.

2. **Существительным с предлогами "при" или “когда”.** When offered work abroad, Popov refused to leave his country. Когда Попову предложили работу за границей, он отказался покинуть свою страну.

3. **"Будучи" + краткая форма причастия**.

Participial Constructions.

Употребление. **Причастные обороты** представляют собой сочетание подлежащего, выраженного существительным или личным местоимением, и какой-либо формы причастия.

The Objective Participial Construction (сложное дополнение). I want it done by 5 o'clock. Я хочу, чтобы это было сделано к 5 часам.

The Absolute Participial Construction (независимый причастный оборот). Независимый причастный оборот отделяется запятой и не связан ни с одним словом в другой части предложения. Он переводится **в начале предложения – обстоятельственным придаточным предложением** с союзами (так как, когда, если), **в конце предложения – простым предложением**, вводящимся союзами (причем, а, и) или бессоюзно. The driver having repaired the motor, we could go further. После того, как водитель отремонтировал мотор, мы смогли двигаться дальше. Независимый причастный оборот может вводиться предлогом **with.** With experiments having been carried

out, we started new investigation. После того, как опыты были произведены, мы начали новые исследования.

APPENDIX 2

Writing an Abstract

Steps.

I. The aim and methods of the research.

II. Characteristics of the research.

III. The results of the work.

Phrases.

1. This paper presents (discusses, illustrates, describes, contrasts, explores, shares one's experience in, investigates, introduces,, seeks to develop, advocates, gives a short overview of)…
2. This paper is an attempt to…
3. In this paper we survey…
4. The author presents (discusses, proposes, studies, generalizes, conceives, has tried to ensure)…
5. The initial purpose of study was…
6. It is pointed out that…
7. It is argued that…
8. Our concern in this paper is to show…
9. Special attention is devoted to…
10. The main focus is on…
11. The effectiveness of this method has been confirmed…
12. The described method is applicable to…
13. The method requires…
14. The method can be regarded as…
15. Finally…
16. Thus…

17. The paper ends with the discussion…
18. Experimental results are presented…
19. The main result is…
20. The results indicate / are presented / based on…
21. Conclusions are drawn
22. The study summarizes the results…
23. The main contribution of the present work is…

APPENDIX 3

a) Chronological resume. George's resume has details about his work experience and coursework that will strengthen his application for the position.

George Amalfi
5001 Lampe Avenue
Consdale, IL 6033(504)347-8432

OBJECTIVE:	Commercial Loan Officer
WORK EXPERIENCE: 1999-present	Commercial Credit Analyst Biggs Bank, Carnsdale, IL Analyze and structure commercial loan packages Develop new business Manage and train junior loan officers Work with domestic clients
EDUCATION: June 2000 June 1996	MBA, France Grandell University, Chicago, IL GPA 3.59 BS Business Administration University of Wisconsin, Madison WI GPA 3.59
COURSEWORK:	Financial management of banking institutions

	Money and banking Quantitative business methods Marketing management International business
HONORS:	Crandell University Fellowship
FOREIGN LANGUAGE:	Fluent in German
INTERESTS:	Triathlete training Photography
REFERENCES:	Available on request

b) Functional resume. Timothy's skills have been derived primarily from clerical positions and from volunteer work. As he is looking for a position as a management trainee, he puts his managerial skills first.

TIMOTHY CHU
309 Fleury Street
St.Paul, MN
38276(022)262353 (day time) (336)47436 (evening)

EDUCATION June 1988	 BS, Management, University of Minnesota GPA 3.38
OBJECTIVE	Management trainee
SKILLS Managerial: Technical:	 Planned fundraising activities for nonprofit corporation Supervised a staff of six clerical workers Organized and facilitated clerical planning group to improve work Organized and conducted aid workshops Handled managerial accounts for small company Estimated data patterns using diverse forecasting methods Have experience with cost benefit analysis Program in MINITAB an BASIC Conducted research project on recidivism rate

Analytical: Communication:	among mentally ill in St.Paul Implemented project to improve communication between management and clerical staff Created system to improve data collection for reports to management
PERSONAL	Willing to relocate
	References on request

c) Combination form resumes. This resume combines skills with chronological information. Arthur puts his academic and professional qualifications at the beginning of the resume and deemphasizes dares. He includes a computer skills section that will be useful for an employer interested in hiring a programmer or analyst.

ARTHUR TOWNE
478 Coy Drive
Hanes, NH 32456
(303)230-1296

JOB OBJECTIVE	Computer programmer/Analyst
QUALIFICATION	BS, Management Information Systems 2 years' full-time programming experience
EXPERIENCE	Programmer, Computerland Boston MA Designed an integrate sales order/purchase order system Designed and implemented accounts receivable system and utilities to work with point-of-sale software. Also worked in sales, customer support, and technical service (1997- 1999).
EDUCATION	BS, Computer Science, Boston College. Mathematics minor (June 1999)
COMPUTER SKILLS	Have worked on IBM PC/XT, IMSAI 8080, Northstar Horizon, HP-2000F, CDC Cyber

	170 720-2 Familiar with UNIX, PC-DOS, Primos, CP/M, NOS.
COURSEWORK	Information Systems Administrations Management Information Systems Technical Writing Business Calculus
MEMBERSHIP	Data Processing Management
REFERENCES	On request

APPENDIX 4

Curriculum Vitae

1. Name Surname
2. Personal Information

Address

Telephone home: mobile:

Nationality

Marital status

Date of birth

Email

3. Career history
4. Education
5. Languages
6. Computer skills
7. Additional information

SAMPLE

PATRICIA HEPWORTH

1 Any Road, Anytown AN1 1CV

Telephone: 01632 960 739 (Home); 07700 900 709 (Mobile)

Email: patriciahepworth@example.com

Professional Profile

A dedicated and results-driven senior manager with a highly successful background in the achievement of profitable business growth through the creation and execution of successful sales and marketing strategies. Experienced in working with leading brands in the competitive retail and automotive industries with the primary focus on exceeding expectations for customer service delivery while ensuring optimum brand impact. Possesses excellent interpersonal, communication and negotiation skills and the ability to develop and maintain mutually beneficial internal and external relationships. Enjoys being part of, as well as managing, motivating and training, a successful and productive team, and thrives in highly pressurised and challenging working environments.

Career Summary

2005–2009 TYRES UK LTD

Freelance Consultant/Interim Network Development Manager

- Project managing the redevelopment of the retail sales strategy across the UK market with the ultimate aim of facilitating business performance improvements
- Successfully developing multi-channel solutions including instigating a new HiQ Fast Fit Franchise proposition
- Playing a pivotal role in the design and development of a class-leading B2C eBusiness website
- Working in close conjunction with external professionals to create and implement a retail network representation plan
- Actively involved in developing a new retail store concept and in redrafting all contractual agreements and process/procedure manuals
- Coordinating the pitch and scoping process for the selection of a staff training and development academy

1999–2005 BDW GROUP

2005–2005 Managing Director, BDW Contact Ltd

- Fully accountable for the establishment and management of a new business arm specialising in the provision of telemarketing services requiring the development of an independent customer base
- Collaborating with professionals and third parties to set up the infrastructure for the company and coordinating the recruitment, selection and training of 15 members of staff
- Planning and organising a highly successful launch programme and driving the business forward to break-even three months ahead of projections
- Introducing a range of B2B and B2C services and facilitating the provision of 24-hour service by business partnership in conjunction with an external agency

2000–2004 Operations Director

- Providing management and support to up to 68 members of staff and motivating them towards the achievement of optimum service delivery standards to facilitate customer satisfaction and maximum revenue generation
- Maintaining full profit and loss accountability up to £5 million while achieving a year-on-year growth in revenue of more than 10%
- Initiating half yearly service reviews with major blue chip, retail clients and formalising account planning to ensure best practice resulting directly in recognition for excellence in customer surveys
- Developing and implementing new billing and forecasting systems which significantly improved overall efficiency
- Enabling a 5% increase in actual gross margin in 1 year through the implementation of a staff incentive scheme

Career Summary cont.

1999–2000 Account Director

- Working in close conjunction with key client representatives to develop marketing strategies and point-of-sale materials on behalf of retail partners
- Negotiating and securing £120,000 in bespoke systems development revenue and playing a key role in increasing monthly revenue from £12,000 to £100,000

1996–1999 WORDS PICTURES SOUNDS

Managing Director

- Setting up and developing a full service design agency from the initial business planning, financial forecasting and business strategy development through to building and retaining the customer base
- Successfully securing and effectively managing contracts with leading brands including Audi, One 2 One and Cadbury for the provision of a range of creative services including media creative, brochure design, corporate identity and hard point of sale
- Achieving approved supplied status with Audi and One 2 One and delivering sustained income growth with the turnover increasing from £75,000 in 1996 to £750,000 in 1999

1983–1996 VAG (UK) LTD

Audi A8 Project Manager

- Commencing employment as a Trainee Field Sales Manager on behalf of the sole importers of Volkswagen and Audi vehicles and parts into the UK
- Gaining a series of promotions through various product, marketing, operations and advertising management positions, both head office and field based
- Ultimately undertaking the head office role of Audi A8 Project Manager tasked with the development and promotion of the brand and the vehicle within the luxury market with a total spend of £1.5 million

Education and Qualifications

4 A Levels Mathematics, Economics, History and General Studies

8 O Levels Including English and Mathematics

Professional Development

- Management Development Programme
- Marketing Management
- Presentation Skills
- Finance for Non-financial Managers
- Effective Man Management
- Appraisal Training
- Team Building
- Creativity Training

IT Skills

- Word, Excel, Access, PowerPoint, Internet and Email

Personal Details

Driving Licence Full/Clean

Health Excellent; non-smoker

Interests Squash, Golf, Reading (current affairs), Theatre and Cuisine

References Are Available On Request

APPENDIX 5

Additional information

1. The Protection of Information in Computer Systems. Jerome H.Saltzer, M.D.Schroeder, www.cs.virginia.edu/~evans/cs551/saltzer/
2. Secure IT. www.e-pag.com/secureit/secure_it_page.htm
3. Business Project Risk Management Analysis. www.risk-analysis-guide.com.
4. Risk Analysis Technicues. www.mindtools.com/pages/article/newTMC_07.htmWelcome to Cryptography. www.cryptography.org
5. Cryptography e-Books. kazus.ru/ebooks/books/eng/22/0/0.html
6. An Overview of Cryptography. www.garykessler.net/library/crypto.html
7. YouTube – Theory and Practice of Cryptography. www.youtube.com.watch?v=ZDnShu5V99s
8. Applied Cryptanalysis: Breaking Ciphers in the Real World. Авторы: Stamp M., Low R.M. lib.mexmat.ru/books/29261
9. YouTube – How to Use Cryptanalysis to Obtain and Decrypt Passwards. www.youtube.com.watch?v=P60JYKtpec8
10. Steganography and Digital Watermarking – Attacks and Countermeasures. www.jjtc.com/stegoarchive/
11. Steganography. www.garykessler.net/library/steganography.html
12. Steganography Tools. www.cotse.com/tools/stega.htm
13. Quantum Cryptography. en.academic.ru/dic.nsf/enwiki/33151
14. Quantum Cryptography. cryptoblog.wordpress.com/
15. Quantum Cryptography and Secret Key Distillation. gva.noekeon.org/QCandSKD/

16. What is Quantum Cryptography? codebetter.com/blogs/raymond.lewallen/archive/
17. Internet Protection. www.symantec.com/reference/
18. Character Link – Strongest Internet Protection. www.characterlink.net
19. BitDefender Internet Security. www.bitdefender.com/solutions/internet
20. Internet Protection Act. www.state.nj.us/njded/techno/htcrime/ipa.htm
21. Data Protection Issues for Intranet Managers.
www.intranetfocus.com/…dataprotection.pdf
22. Virus Protection and Hostile Applets.
www.podgoretsky.com/ftp/Docs/Internet…Intranets…
23. Intranets – Table of Contents. www.bookrags.com/research/intranet-csci-04/
24. Fact Sheet: Reforms to Protect American Credit Card Holders.
www.whitehouse.gov/the_press_office…Credit-Card
25. Credit Card Protection. www.credit-land.com/articles/articles_page_68600_
26. Firewalls: Firewalls Review. www.consumersearch.com/firewalls

Word list

Unit 1

administrative and legal framework – административно-правовая структура (основа)

applications – приложения

assurance measures – средства обеспечения доверия

availability - доступность

carry out – проводить. выполнять

confidentiality - конфиденциальность

conformance – соответствие, согласованность

consumer – потребитель

counter the identified threats – противопоставить установленным угрозам

developer – разработчик

distributed systems – распределенные системы

evaluator – оценщик

electromagnetic emanation control – контроль электромагнитного излучения

firmware – программно-аппаратное обеспечение, встроенные программы

form judgements – составить мнение

fulfill the needs – удовлетворять потребности

fundamental purpose and justification – основная цель и оправдание (подтверждение)

hardware – аппаратное обеспечение

have an impact – иметь последствия

implement – осуществлять, выполнять

implementation-independent structure – структура, не зависящая от реализации

implicit – скрытый, неявный

inherent qualities – специфические (неотъемлемые / встроенные свойства)

integrity - целостность

loss of use – потеря возможности использования

make claims – утверждать

malicious – злонамеренный, злоумышленный

meet the requirements – отвечать требованиям

modification – изменение

non-human threats – угрозы, исходящие не от человека

oversight – контроль, надзор

procurement – приобретение

Protection Profile – профиль защиты

secure usage assumptions – предположения безопасного использования

security evaluation – оценка безопасности

security property – свойство безопасности

security risk – риск нарушения ИБ

Security Target – задание по безопасности

software – программное обеспечение

system custodian – системный администратор

Target of Evaluation (TOE) - объект оценки

threat - угроза

tolerable – допустимый, приемлемый

types of failure of security – типы нарушения безопасности

unauthorized disclosure – несанкционированное раскрытие

Unit 2

Adversary – злоумышленник

access delay – задержка доступа

access point – точка доступа

acceptable risk – приемлемый риск

assess risk – оценить риск

bypass each delay element - блокировать каждый задержанный элемент

commit an act/event – совершить действие

consequence definition – определение последствий

delay an adversary – воспрепятствовать злоумышленнику

deployment of the response force – применение ответных сил

detect an adversary – обнаружить злоумышленника

entry control – контроль входа

environmental impact statement – заключение о влиянии на окружающую среду

equation – уравнение, равенство

estimate risk – оценить риск

estimation of likelihood of attack – оценка вероятности атаки

facility - объект

facility design blueprint – схема объекта (на кальке)

fault tree – дерево ошибок

intrusion – вторжение

likelihood of adversary attacks – вероятность злоумышленных атак

local/state/federal law enforcement – принудительное осуществление закона

modus operandi – план, способ действия

protection objective – цель защиты

reduce risk – уменьшить риск

respective critical asset – активы с предполагаемой подверженностью риску

response force – сила ответных действий

retrofit - модифицированная модель, усовершенствованная конструкция

safeguards functions – функции мер безопасности

severe environmental damage – серьезный ущерб окружающей среде

sense a covert/overt action – обнаружить тайное/явное действие

site boundary – границы участка

site survey – исследование территории

target - цель

threat - угроза

total mission loss – абсолютная невозможность выполнять свои функции

unacceptable risk – неприемлемый риск

undesired event – нежелательное событие

vulnerability analysis – анализ уязвимости

Unit 3

Adjustment – дополнение, приложение

authenticate information – подтвердить подлинность информации

be exploitable into an attack – использоваться для атаки

brute force (attack) – атака методом перебора

bulk data – массив данных

cipher block chaining - сцепление блоков шифртекста

ciphertext - шифртекст

communicating host – хост связи

decryption - расшифрование

digital signature - электронно-цифровая подпись

discard the bytes – исключить байты

eavesdropper – злоумышленник, подслушивающее устройство

elliptic curve cryptography - криптография на основе эллиптических кривых

encryption - шифрование

factorization algorithm - алгоритм разложения на простые множители

flexibility – гибкость (применения), оперативность

implementation - реализация

incompatible standards – несовместимые стандарты

initialization vector – вектор инициализации

integrity protection – защита целостности

keyring server – сервер ключей

man-in-the middle-attack – атака «человек-в-середине»

optional authentication of the client – дополнительная аутентификация клиента

parity bit – бит четности

plaintext – открытый / незашифрованный текст

random padding – произвольное дополнение незначащей информацией или фиктивными битами, холостое заполнение

secure an application – обеспечить безопасность приложения

small-ability smartcard – малофункциональная смарткарта

standard-conforming protocol – протокол стандартного соответствия

string of binary – строка двоичного кода

suite of tools – набор инструментов (средств)

withstand an attack – противостоять/выдержать атаку

Unit 4

automated aids – автоматические вспомогательные средства

avalanche property of DES – лавинное свойство алгоритма DES

brute-force search - исчерпывающий поиск, поиск методом перебора

calculus – исчисление, дифференциальное и интегральное исчисление, математический анализ

chain of discrete elements – цепочка дискретных элементов

ciphertext-only solution – решение, основанное только на имеющемся зашифрованном тексте

converted unit record equipment (punched card machines) - счётно-перфорационная машина, счётно-аналитическая машина

encipher the known plaintext – зашифровать известный открытый текст

flaw – изъян, дефект, слабое место

flipped bit results – результаты инвертирования битов

higher-order differential - дифференциал высшего порядка

hill climbing algorithm – алгоритм нахождения экстремума

incomprehensible ciphertext – непонятный шифртекст

linear cryptanalysis – линейный криптоанализ

mimic the process (of natural selection) – имитировать процесс (естественного отбора)

obtain clue – получить ключ

(original) trial key – (первоначальный) пробный ключ

overlapping superencipherment group – совпадающие шифровальные группы

recover a DES key – восстановить ключ DES

remove a bit of drudgery – снять часть тяжелой, монотонной работы

second-order derivative - производная второго порядка

subkey - подключ

trial encipherment – пробное шифрование

truncated differential – отсеченный дифференциал

unrelated characteristics - несвязанные характеристики

xor – исключающее «или» (мат.)

Unit 5

bit-for-bit identical – поразрядно идентичный

carrier text – текст-носитель зашифрованной информации

coin a term – ввести термин

convey a message – передавать сообщение

covered (concealment) cipher – скрытый шифр

covert communication – скрытое общение

cue code – сигнальный код

date back – датироваться, вести начало от к-л даты

digital watermarking – нанесение цифровых водяных знаков

discrete cosine transforms coefficient – коэффициент дискретного косинусного преобразования

doodle – черточка, дополнительный штрих в букве

embed – внедрять, встраивать

financial fraud – финансовое мошенничество

font - шрифт

formatting vagary – разновидность форматирования

grille cipher – трафаретный шифр

in nonobvious way – скрыто, неявно

intend - намереваться

lossy compression - сжатие с потерей данных

microdot - микрофотоснимок

nefarious application – использование в незаконных целях

overt communication – открытое общение

party – сторона (общения)

proprietary compression scheme – патентованная схема упаковки

pulse code modulation - кодово-импульсная модуляция

retrieve the hidden text – восстановить (извлечь) скрытый текст

size-reduction method – метод уменьшения размера

spam mimic – имитация спама

staple – главный элемент

steganography medium – стеганографическая среда

template - шаблон

treat - рассматривать

warchalking – нанесение меток

Unit 6

allow through - пропускать

angle - угол

be bugged - быть под тайным наблюдением

be a bit off – быть слегка измененным (об угле поляризационного фильтра)

be on the lunatic fringe (of cryptography) – быть на периферии (криптографии)

collapse - разрушиться

discard the bits - отвергнуть биты

discrepancy - расхождение

eavesdrop - подслушивать

expand on an idea – развить мысль

guess - угадать

match a filter – подстраиваться под фильтр

measure (v) - измерять

over an insecure channel – через незащищенный канал

parity of subsets - сравнимость подмножеств по модулю

polarization filter - поляризационный фильтр

prearranged code – заранее условленный код

quantum key distribution – распределение квантового ключа

qubit – кубит, единица квантовой информации, квантовый аналог классического бита

random result – случайный результат

rectilinear polarization – линейная поляризация

string of photon pulses – последовательность фотонных импульсов

Unit 7

embedding of a program – внедрение программы

enciphering - криптографическая защита, шифрование

general security complex – комплекс общей безопасности

increase functioning effectiveness – увеличить эффективность работы

information safety assurance – обеспечение информационной безопасности

integrity - целостность

intrusion - вторжение

offer the required flexibility – обеспечить необходимую гибкость

penetration - проникновение

program and hardware protecting tools – средства защиты программного и аппаратного обеспечения

proof algorithm for random numbers generation – надежный алгоритм для получения случайных чисел

reveal and prevent possible UAA threats – выявлять и предотвращать возможные угрозы несанкционированного доступа

shortcomings of an approach – недостатки подхода

smart-attack – направленная, сгенерированная атака

take into account – принимать во внимание

take a significant place – занимать важное место

unauthorized user – незаконный пользователь

vulnerable network components definition and protection – определение и защита уязвимых компонентов сети

Unit 8

application session –соединение приложений

blocking identity spoofing - блокирование маскировки злоумышленника под законного пользователя

blocking snooping – блокирование слежения

data theft – кража данных

dedicated private line – частная сеть для специальных целей

digital signature – цифровая подпись

external risk – риск нарушения ИБ извне

implement a security policy – реализовывать политику безопасности

internal risk - риск нарушения ИБ изнутри

intranet publishing guideline – руководство по пользованию корпоративной сетью

iris pattern – узор, изображение радужной оболочки глаза

malware – обеспечение, созданное со злым умыслом

misconception – неправильное понимание

network stack - стековое запоминающее устройство

one-time password – одноразовый пароль

packet sniffing - контроль сообщений, передаваемых по сети связи, с целью выявления конфиденциальной информации

port forwarding - передача на мобильную радиотелефонную станцию

proactive - профилактический, предупреждающий

proprietary data - собственные данные

reactive – реагирующий на случившееся

remote intranet access – удаленный доступ к корпоративной сети

repository - хранилище

retinal pattern – изображение сетчатки глаза, узор сетчатки глаза

reusable password – многоразовый пароль

security breach – нарушение безопасности

security outsourcing – использование дополнительных средств безопасности извне

Secure Sockets Layer - протокол защищенных сокетов (протокол, гарантирующий безопасную передачу данных по сети; комбинирует криптографическую систему с открытым ключом и блочное шифрование данных)

thin client laptop – компьютер простого клиента

Unit 9

application layer - прикладной уровень

chart a table of filtering rules – составить таблицу правил фильтрации

choke point principle – индукторный точечный принцип

collapsed network - рухнувшая сеть

data link layer - канальный уровень

default failure mode – вид отказа по умолчанию

destination port - порт получателя

distributed firewall – распределенный межсетевой экран

dual homed gateway - двухпортовой шлюз

flaw in the Web server – дефект, слабое место в сервере

functional layer – функциональный уровень

gate – пропускать

gateway – шлюз

hardware firewall – аппаратный межсетевой экран

information outflow - утечка информации

information traffic – движение информации

mediator - посредник

net configuration – конфигурация сети

network layer - сетевой уровень

OSI model - модель взаимодействия открытых систем (семиуровневая модель протоколов передачи данных в открытых системах)

outside hub - внешний узел

packet filter – фильтр пакетов

packet proceeding – обработка пакетов

representation layer - уровень представления

router - маршрутный прокладчик, маршрутизатор

screened gateway – защищенный сетевым экраном (межсетевой) шлюз

screened subnet – защищенная сетевым экраном подсеть

screening router - экранирующий маршрутизатор

session layer - сеансовый уровень

software firewall – программный межсетевой экран

source port - порт отправителя

Unit 10

ad hoc network – произвольно создаваемая сеть

assets (of an enterprise) – активы (предприятия)

bandwidth – полоса пропускания

circuit switched – подключенный к цепи

cordless system – беспроводная система

cross-building interconnect – соединение в пределах здания

data rate – скорость, интенсивность прохождения данных

fail-over – провал, неудача, сбой

flow control - контроль передачи, управление потоком данных

gateway - межсетевой шлюз

handover delay – задержка перемещения вызова

inbound traffic – трафик входящих сообщений

intruder - лицо, не имеющее санкционированного доступа

low power consumption – низкое потребление энергии

malicious intent - злой умысел

node - коммутатор

nomadic access – удаленный доступ

outbound traffic - трафик исходящих сообщений

overlap - совпадение

personal digital assistant (PDA) персональный цифровой секретарь (карманный компьютер, используемый в качестве записной книжки)

protocol conversion - преобразование протоколов

security compromise – соглашение о безопасности

spoof – обманывать

statically-assigned IP address – статистически назначенный адрес

two-way radio – приемно-передающая радиоустановка

Wireless Local Area Network – локальная беспроводная сеть

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. English for computer science students: Учебное пособие / Сост. Т.В.Смирнова, М.В.Юдельсон; Науч.ред. Н.А.Дударева. – 3-е изд. – М.: Флинта: Наука, 2003.

2. ГОСТ Р ИСО/МЭК 15408-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. – М.: Изд-во стандартов, 2002.

3. Рубцова М.Г. Чтение и перевод английской научной и технической литературы: Лексико-грамматический справочник / М.Г.Рубцова. – 2-е изд. испр. и доп. – М.: ООО «Издательство АСТ»: ООО «Издательство Астрель», 2004, – 384с.

4. Гольцова Е.В.Английский язык для пользователей ПК и программистов: Самоучитель. – 3-е изд. – СПб.: КОРОНА принт; М.: БИНОМ пресс, 2004. – 480.

5. Судовцев В.А. Учись читать литературу по специальности. (Английский язык): Учеб. пособие для студентов техн. Вузов, обучающихся по радиотехническим спец. и спец. связи. – М.: Высш. школа, 1985. – 112 с.

6. Мельник О.Г., Тарасенко О.С., Нечаева Т.А., Краснощекова Г.А. The non-finite forms of the verb. – Таганрог: ТРТУ, 2001

7. Балуян С.Р. Are you looking for a job. – Таганрог: ТРТУ, 2003. – 80 с.

8. Практические правила управления информационной безопасностью. ISO/IEC 17799:2000. Information Technology. Code of practice for information security management. – Printed in Switzerland: ISO/IEC 2000.

9. Общие критерии оценки безопасности информационных технологий. ISO/IEC 15408-1:1999. Information Technology. Security techniques. Evaluation criteria for IT security. – Part 1, 62 p. – Part 2, 360 p. – Part 3, 214 p.

10. Руководство по разработке профилей защиты и заданий по безопасности. ISO/IEC 15446: 2000. Information technology. Security techniques. Guide for the production of protection profiles and security targets. – 156 p.

11. CC Profiling Knowledge Base™. User Guide. Profiling Assumptions, Threats, and Policies. Through Objectives to Requirements. Version 1.0 j, k. – NIAP, May, 2000. (http://niap.nist.gov/tools/cctool.html).

12. Reference guide to fiber optic testing. Volume 1. JDS Uniphase corporation. 2007.

13. **CustomerServices@ineedacv.co.uk**

Учебное пособие

Сальная Лейла Климентьевна

Secure IT

Ответственный за выпуск Сальная Л.К.

Редакторы: Кочергина Т.Ф., Проценко И.А.

ЛР № 020565 от 23.06.1997 г. Подписано к печати г.

Формат 60x84/ $^{1}/_{16}$

Бумага офсетная Печать офсетная

Усл. п. л. – 13,9 Уч.-изд.л. – 13,9

Тираж 150 экз. Заказ №

«С»

Издательство Технологического института
Южного федерального университета
ГСП 17 А, Таганрог, 28, Некрасовский, 44

Типография Технологического института
Южного федерального университета
ГСП 17 А, Таганрог, 28, Энгельса, 1