Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный технический университет имени Н.Э. Баумана
(национальный исследовательский университет)»
(МГТУ им. Н.Э. Баумана)

Е.С. Ражева, Е.А. Смелкова, О.В. Трошина

ENGLISH FOR INFORMATION SECURITY SPECIALISTS

АНГЛИЙСКИЙ ЯЗЫК ДЛЯ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебное пособие

для студентов 3 курса, обучающихся по специальности «Информационная безопасность», квалификация (степень) «инженер»

Москва
Издательство МГТУ им. Н.Э. Баумана
2019

УДК 81: 378(075)

ББК 81.2 Англ

Рекомендовано Редакционно-издательским советом

МГТУ им. Н.Э. Баумана в качестве учебного пособия

Рецензент

Ражева, Е.С., Смелкова, Е.А., Трошина, О.В.

English for Information Security Specialists: Английский язык для специалистов в области информационной безопасности. Учебное пособие для студентов 3 курса, обучающихся по специальности «Информационная безопасность», квалификация (степень) «инженер». – Москва: Издательство МГТУ им. Н.Э. Баумана, 2019. – 118с.

ISBN……..

Ц27 Учебное пособие предназначено для основной и дополнительной работы студентов третьего курса над профессионально-ориентированным английским языком по дисциплине «Информационная безопасность». Пособие состоит из двух основных модулей, глоссария и приложения, предназначенного для повторения ранее пройденного материала и подготовки к экзамену. Каждый из модулей включает аутентичные англоязычные материалы по актуальным темам, включая угрозы информационной безопасности и защиту информации. Поурочный терминологический словарь помогает усвоению лексики по изучаемой тематике. На базе аутентичных текстов профессиональной направленности созданы лексические и грамматические упражнения, задания на развитие комплекса навыков: чтения, устной речи, письма, аудирования, критического мышления, а также на интерактивные виды учебной работы (ролевые игры, решение кейс-задач).

© Ражева, Е.С., Смелкова, Е.А., Трошина, О.В., 2019

© МГТУ им. Н.Э. Баумана, 2019

© Оформление. Издательство МГТУ им. Н.Э. Баумана, 2019

ISBN……..

В соответствии со ст. 1299 и 1301 ГК РФ при устранении ограничений, установленных техническими средствами защиты авторских прав, правообладатель вправе требовать от нарушителя возмещения убытков или выплаты компенсации.

Оглавление

ПРЕДИСЛОВИЕ

Учебное пособие создано для основной и дополнительной работы студентов 3-его курса (аудиторной, внеаудиторной и самостоятельной), обучающихся по специальности 10.03.01 «Информационная безопасность» (квалификация – специалист по информационной безопасности), над профильно-ориентированным английским языком в рамках дисциплины «Иностранный (английский) язык».

Цель изучения дисциплины – развитие у студентов иноязычной коммуникативный компетенции на таком уровне, который необходим для международного взаимодействия и сотрудничества, освоение базовых принципов функционирования английского языка в профессиональной среде, Приобретение навыков и умений работать с научно-технической литературой и умение понимать лекции научного характера на слух. Все вышеперечисленное должно способствовать успешной профессиональной деятельности.

Планируемые результаты обучения. После изучения дисциплины студенты должны уметь:

- читать, переводить и анализировать аутентичные тексты деловой и профессиональной направленности в сфере информационной безопасности;

-использовать базовые лексические, грамматические, стилистические англоязычные языковые средства в области делового / профессионального устного и письменного общения на английском языке в сфере информационной безопасности;

- составлять монологические и диалогические высказывания, а также участвовать в дискуссиях, диспутах, полемиках, круглых столах, ролевых играх на деловые и профессиональные темы в сфере информационной безопасности;

- выполнять лексико-грамматические и терминологические тестовые

задания на основе профессионально-ориентированного англоязычного материала по темам, связанным с информационной безопасностью;

- владеть основными навыками устной публичной речи, аргументации, подготовки и выступления с презентацией на английском языке;

- решать проблемные задания (кейса), связанные с информационной безопасностью.

Учебное пособие, как и дисциплина, состоит из модулей, каждый из модулей представляет собой логически-завершенный раздел курса. Каждый модуль имеет в своем составе поурочный терминологический словарь, упражнения, направленные на развитие лексических, грамматических навыков, а также задания на развитие навыков чтения, говорения, аудирования и письма. Интерактивные виды деятельности также включены в каждый модуль: кейс-задачи и ролевые игры. Данные упражнения и задания помогают развивать все основные виды деятельности на английском языке. В пособии к каждому модулю даются тренировочные упражнения на подготовку к экзамену, а приложения дают возможность повторить материал. Материалы пособия имеют практико-ориентированный характер, обеспечивая возможность решения конкретных практических профессиональных задач, связанных с целью и планируемыми результатами обучения по дисциплине.

Методика проработки и освоения материала модулей дисциплины

Дисциплина предназначена для достижения результатов обучения, которые указывают на то, что студент должен будет после освоения дисциплины *знать* (помнить и понимать), *уметь* (применять, анализировать, оценивать, создавать), какими важными навыками он должен *овладеть*. Планируемые результаты обучения сформулированы в программе дисциплины «Иностранный (английский) язык.

На первом занятии каждый студент получает в электронном виде полный комплект учебно-методических материалов по дисциплине,

включающий программу, учебное пособие, дополнительные справочные и учебные пособия, рекомендуемые для самостоятельной проработки программы курса и подготовки к промежуточной аттестации в виде экзамена.

Семинарские занятия являются основным видом аудиторной учебной деятельности студентов в рамках дисциплины «Иностранный язык», на которых студенты изучают ключевые, базовые положения курса, тренируют основные виды речевой деятельности (чтение, говорение, письмо, аудирование), приобретают навыки эффективного межкультурного общения в сфере профессиональной деятельности. Особое внимание уделяется умению понимать и критически анализировать аутентичные англоязычные тексты, извлекать необходимую информацию и обмениваться ею, составляя связанные аргументированные высказывания в условно-реальных ситуациях общения.

Самостоятельная работа студентов включает проработку материалов аудиторных занятий, аналитическое чтение профессионально-ориентированных текстов, выполнение заданий на отработку лексико-грамматических единиц и структур в пределах тем модулей, а также задания на формирование навыков письменной речи (эссе, аннотаций, личных и деловых писем), задания для решения кейс задач (кейс-стади). Каждый раздел завершается контрольными заданиями, которые необходимо проработать самостоятельно, учитывая, что аналогичные задания будут предложены при рубежном контроле усвоения каждого модуля дисциплины.

Текущий контроль проводится в течение каждого модуля**,** его итоговые результаты складываются из следующих оценок:

- *рубежный контроль*, включающий выполнение лексико-грамматического теста, заданий на чтение и проверку понимания содержания прочитанного текста, выступление с монологическим высказыванием по темам модуля;

- *работа на семинарских занятиях*, включающая выполнение заданий по следующим аспектам формирования англоязычных коммуникативных компетенций: чтение и проверка понимания содержания текстов модуля; лексико-грамматических заданий; аудирование; формирование умений и навыков устной речи: диалогической речи (задания для проблемной дискуссии, полемики, диспута, дебатов, круглого стола; подготовка и участие в ролевой и деловой игре); монологической речи (выступление с докладом, сообщением, презентацией);

- *самостоятельная работа студента*: отчет о выполнении дополнительных упражнений на проработку лексико-грамматического материала модуля, выполнение письменных работ, презентация результатов решения кейс задач.

Выполнение всех трех форм текущего контроля результатов обучения является обязательным. Студент должен выполнить все контрольные мероприятия, предусмотренные в модуле учебной дисциплины к указанному сроку. Контрольное мероприятие считается выполненным, если за него студент получил оценку в баллах не ниже минимальной оценки, установленной программой дисциплины по данному мероприятию. Студенты, не сдавшие контрольное мероприятие в установленный срок, продолжают работать над ним в соответствии с порядком, принятым кафедрой.

Промежуточная аттестация по дисциплине (экзамен) основывается на результатах текущего контроля, а также включает дополнительное контрольное мероприятие. Контрольные задания для проверки ключевых результатов обучения по дисциплине обеспечивают возможность объективной независимой оценки знаний, умений и навыков, приобретенных студентом.

Освоение дисциплины, ее успешное завершение на стадии промежуточного контроля (экзамена) возможно только при регулярной работе во время семестра и планомерном прохождении текущего контроля.

ВВЕДЕНИЕ

Иностранный язык на сегодняшний день можно назвать неотъемлемой частью подготовки специалистов с высокой квалификацией в неязыковых вузах. Несомненно, что погружение в среду иностранного языка помогает развитию профессиональных компетенций и самообразованию. В данном случае просто необходимы навыки нахождения и применения современных знаний и открытий в научной сфере. Более того, неоспоримо, что умение пользоваться иностранным языком в современном мире стало обязательным условием ведения успешной профессиональной деятельности.

Актуальность разработки и издания настоящего учебного пособия обусловлена недостаточной разработанной базы аутентичного и идущего в ногу со временем материала для формирования и развития коммуникативных компетенций в структуре профессиональной компетентности будущих специалистов в области информационной безопасности. Специально подобранный аутентичный материал позволяет студентам работать с действительно актуальными единицами как языкового, так и коммуникативного уровня, использующимися в их специальности. Учебное пособие прошло успешную апробацию среди студентов 3-его курса, обучающихся на кафедре «Информационная безопасность» МГТУ им. Н.Э. Баумана, в 2017-2018 учебном году, что позволило усовершенствовать его содержание с учетом мнений и пожеланий студентов и преподавателей.

Учебное пособие отвечает последним требованиям, предъявляемым к изданиям такого рода. Поурочный терминологический словарь помогает усвоению лексики по изучаемой тематике. На базе аутентичных текстов профессиональной направленности созданы лексические и грамматические упражнения, задания на развитие комплекса навыков: чтения, устной речи, письма, аудирования, критического мышления, а также на интерактивные

виды учебной работы (ролевые игры, решение кейс-задач), что в свою очередь, развивает у студентов не только иноязычную коммуникативную компетенцию, но и стремление к познавательной деятельности через повышение мотивации.

Практическая значимость предлагаемого учебного пособия состоит в реализации главной задачи дисциплины «Иностранный (английский) язык» на третьем курсе обучения МГТУ им. Н.Э. Баумана, которая заключается в формировании у студентов иноязычной коммуникативной компетенции как основы профессиональной деятельности на иностранном языке.

Учебное пособие нацелено на закрепление и совершенствование всех видов речевой деятельности, которые представляют собой чтение, аудирование, говорение и письмо). То есть данное пособие представляет собой переход от общенаучной сферы коммуникации (1 и 2 курсы обучения) к узкоспециальной (3 курс).

Предметная (содержательная) характеристика учебной дисциплины. Трудоемкость дисциплины «Иностранный язык» на третьем курсе составляет 4 зачетные единицы или 144 академических часа, включающих 68 аудиторных часов и 76 часов самостоятельной работы.

Учебное пособие соответствует рабочей программе «Иностранный язык» по специальности 10.03.01 «Информационная безопасность» (квалификация (степень) «инженер») и рассчитано на аудиторную и самостоятельную работу студентов в пределах выше обозначенных часов.

Тематика модулей соотносится с рабочей программой дисциплины и аутентичный материал пособия отобран таким образом, что подойдет для студентов с уровнем владения языка выше среднего. Преподаватели, использующие данное пособие, могут по своему усмотрению либо упрощать материал для студентов с более слабыми знаниями, либо усложнять для студентов, чей уровень владения языком считается продвинутым.

Структура курса. Пособие состоит из двух основных модулей и приложения, предназначенного для повторения ранее пройденного материала и подготовки к экзамену. Первые два модуля состоят из первого опорного текста (1A, 2A), разделов Language Focus (работа с лексикой), Listening (основаны на лекциях Tedtalks), Writing, Case Study, Grammar, Role-Play, текстов ознакомительного характера (1B, 1C, 2B, 2C) и раздела Assignments for Self-Evaluation: Examination Paper Sample, в котором содержатся задания в формате экзамена. В конце пособия даются приложения: одно направленно на дополнительные материалы для подготовки к экзамену, в другом даются готовые темы для экзамена.

Первый модуль «Information Security Procedure» направлен на освещение проблемы информационной безопасности, рассматриваются типы угроз в общем, и в частности обсуждаются облачные угрозы и угрозы мобильных устройств. В разделе посвященному письму студентам предлагается написать аннотацию к предложенной статье и поделиться своим личным опытом столкновения с киберпреступлениями в реальной жизни.

Второй модуль «Standards and Specifications in the fields of Information Security» посвящен искусству взлома и обмана. В разделе Письмо студентам предлагается пошаговая инструкция написания эссе, даются примеры, и предлагается написать эссе на предложенную тему.

УСЛОВНЫЕ ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

adj. – adjective

adv. – adverb

Fig. – figure

n. – noun

v. – verb

Unit 16 Information Security Procedure

Warm up

1. What stories do you think followed these headlines? Compare answers within your group.
    1. Young Cracker on the Run.
    2. From Phone Phreaker to Hacker.
    3. Teaching Spam and Spyware at University.
2. What other types of security threats do you know? Make a list within your group.
3. Study this diagram which depicts primary classes of threats to network security. Try to answer these questions.
    1. What do external threats consist of?
    2. Where do internal threats come from?
    3. What or who can do the most serious damage to a company?
    4. How can a system be protected from sophisticated hacking techniques?

Reading

1A. Type of Security Threats

Vocabulary

property n. – собственность, имущество

theft n. – воровство, кража

corruption n. – повреждение

accessible adj. – доступный

productive adj. – полезный

intended users – предполагаемые пользователи

sensitive adj. – важный, конфиденциальный

valuable adj. – ценный

respectively ad. – соответственно

ubiquitous adj. – вездесущий, повсеместный

penetration n. – проникновение

grapple v. – бороться, пытаться разрешить

vulnerability n. – уязвимость

realm n. – область, сфера

lack n. – недостаток, нехватка

solid adj. – зд. глубокий

range n. – ряд

large-scale adj. – крупный, большой

common adj. –обычный

alter v. – изменять

replicate v. – копировать

execute v. – выполняться

spyware n. - шпионская программа

monitor v. – просматривать

install v. – устанавливать

consent n. – согласие, разрешение

wealth n. – обилие

combat v. – оказывать противодействие

masquerade v. – выдавать себя за кого-то, притворяться

fraudulent adj. - мошеннический

instant message – мгновенное сообщение

entice v. – увлекать, заманивать

inadvertently ad. – непреднамеренно, без умысла

target n. – цель

malicious adj. – вредоносный

bug n. – ошибка, сбой

trick v. – обманывать, провести

reveal v. – рассекретить

amend v. – исправлять, изменять

metadata n. – метаданные, данные о данных

plaintext–открытый текст, нешифрованный

bluesnarfing n. – подключение к блютуз устройству для кражи данных

1. Read the article and choose from the list A-K the word or the collocation which best fits each gap (1-10) in the article. There is one extra collocation which you do not need to use. There is an example at the beginning (0).

0 -C is a branch of computer technology known as information security as applied to computers and networks. The objective of online security includes protection of information and property from theft, corruption, or threats attack, while allowing the information and property to remain accessible and productive to its intended users. The term online system security means the collective processes and mechanisms by which sensitive and valuable information and services are protected from publication, tampering or collapse by unauthorized activities or untrustworthy individuals and unplanned events respectively.

1- Is more and more ubiquitous; the penetration of computer in society is a welcome step towards modernization but society needs to be better equipped to grapple with challenges associated with technology. New hacking techniques are used to penetrate in the network and the security vulnerabilities which are not often discovered create difficulty for the security professionals in order to catch hackers. The difficulties of staying up to date with security issues within the realm of IT education are due to the lack of current information. The recent research is focused on bringing quality security training combined with rapidly changing technology. Online networking security is to provide a solid understanding of the main issues related to security in modern networked computer systems. This covers underlying concepts and foundations of computer security, basic knowledge about security-relevant decisions in designing IT infrastructures, techniques to secure complex systems and practical skills in managing a range of systems, from personal laptop to large-scale infrastructures. There are some common Threats to attack the system:

2- Threat, a computer virus is a program written to alter the way a computer operates, without the permission or knowledge of the user. A virus replicates and executes itself, usually doing damage to your computer in the process.

3- A serious computer security threat, spyware is any program that monitors your online activities or installs programs without your consent for profit or to capture personal information. We've amassed a wealth of knowledge that will help you combat spyware threats and stay safe online.

4- Masquerading as a trustworthy person or business, phishers attempt to steal sensitive financial or personal information through fraudulent email or instant messages. Internet Based Attacks While your computer is connected to the Internet it can be subject to attack through your network communications.

5- Users can be enticed, often by email messages, to visit web sites that contain viruses or Trojans. These sites are known as viral web sites and are often made to look like well-known web sites and can have similar web addresses to the sites they are imitating. Users who visit these sites often inadvertently

download and run a virus or Trojan and can then become infected or the subject of hacker attacks.

6- are often installed with other programs, usually without your knowledge. They record your behaviors on the Internet, display targeted ads to you and can even download other malicious software on to your computer. They are often included within programs that you can download free from the Internet or that are on CDs given away free by magazines. Spyware doesn't usually carry viruses but it can use your system resources and slow down your Internet connection with the display of ads. If the Spyware contains bugs (faults) it can make your computer unstable but the main concern is your privacy. These programs record every step that you take on the Internet.

7- a wireless access point, e.g. an ADSL (Broadband) Router, hasn't been secured then anyone with a wireless device (laptop, PDA, etc.) will be able to connect to it and thereby access the Internet and all the other computers on the wireless network.

8- The act of stealing personal data, specifically calendar and contact information, from a Bluetooth enabled device.

9- ricking computer users into revealing computer security or private information, e.g. passwords, email addresses, etc., by exploiting the natural tendency of a person to trust and/or by exploiting a person's emotional response.

10- The average Microsoft Word, Excel, etc. document includes hidden metadata with details of who created it, who has worked on it, when it has been amended and quite possibly the text of all those changes as well. Viewing a Word document in a text editor can reveal the metadata in plain text at the start and finish of the document.

A Spyware Threats

B Computer Technology

C Security

D Virus Threats

E Virtual Web Sites

F Phishing Threats

G Spyware, Adware and Advertising Trojans

H Social Engineering

I Bluesnarfing

J Microsoft Office Document Metadata

K Unsecured Wireless Access Points

2. In pairs, look at the highlighted words in the article and try to explain them.

3. Match the words. Make sentences using them.

A	B
capture	person
do	information
intended	vulnerability
sensitive	user
security	email
instant	software
fraudulent	text
malicious	message
plain	program
trustworthy	damage
install	information

4. Here are some phrases from the article you have just read. Choose the correct meaning of the phrase.

1…sensitive and valuable information and services are protected …

a. confidential information might be defended
b. tender people might be protected

2A virus replicates…

a. a virus disappears
b. a virus reproduces itself

3Tricking computer users into revealing computer security…

a. making users to tell smb. their passwords etc.
b. making users to crack other people's passwords

4…can reveal the metadata in plain text…

a. in not cyphered text
b. in a simple text, not difficult

5Computer technology is more and more ubiquitous…

a. it is well-known
b. it is wide-spread

6Masquerading as a trustworthy person or business…

a. Looking like a trustworthy person or business
b. Hiding a good person or business

Language Focus

1. Identify the Internet crime sentences (1-6) refer to. Then match them with the advice below (a-f).

scam Trojan horse worm piracy phishing cyberstalking

1 Crackers try to find a way to copy the latest game or computer program.

2 A study has revealed that half a million people will automatically open an email they believe to be from their bank and happy send off all their security details.

3 This software's danger is hidden behind an attractive appearance. That's why it is often wrapped in attractive packages promising photos of celebrities like Anna Kurnikova or Jennifer Lopez.

4 There is a particular danger in Internet commerce and emails. Many people believe they have been offered a special gift only to find out later they have been deceived.

5 'Nimba' spread by sending infected emails and is also able to infect websites, so when a user visits a compromised website, the browser can infect the computer.

6 Every day, millions of children spend time in Internet chat rooms talking with strangers. But what many of them don't realize is that some of the surfers chatting with them may be sexual predators (сексуальныйманьяк).

A People shouldn't buy cracked software or download music illegally from the Internet.

b Be suspicious of wonderful offers. Don't buy if you aren't sure.

c It's dangerous to give personal information to people you contact in chat rooms.

d Don't open attachments from people you don't know even if the subject looks attractive.

e Scan your email and be careful about which websites you visit.

f Check with your bank before sending information.

2. Fill in the gaps in these security tips with words from the box.

digital certificate	malware	virus	scanner	spyware	firewall

antivirus

Malicious software,(1)……., can be avoided by following some basic rules.

Internet users who like cybershopping should get a (2)……, an electronic identity card.

To prevent crackers from breaking into your internal network and obtaining your data, install a (3)…… It will protect you from (4)……..

If you have been hit by a (5)……., don't panic. Download a clean-up utility and always remember to use an (6)…….. program, for example, a virus (7)…….

You and computers

1. What do you do to prevent computer infections?
2. Do you keep your virus protection updated? The Internet has lots of websites where you can get free advice and software. What should you do to improve your computer security?

Listening

All Your Devices can be Hacked

1. You'll watch the video the possibility of hacking different devices. Try to catch the general idea.

2. Watch the first part of the video again. Fill each gap in this summary with ONE word only.

1 I'm a computer science professor, and my area of expertise is computer and ……. security.

2 Apparently, I was in ……. of making sure that no …… stole the computers from the university.

3 And I'm not a doctor, but I reassured her that it was very, very …… that this would happen, but if she felt more comfortable, she could be free to use …… gloves when she was on the computer, and there would be no harm whatsoever in that.

4 It's all work that my colleagues have done, and I actually asked them for their slides and …….. them into this talk.

5 Because that's when …….. devices inside of people started to have …….. capabilities.

6 Now what a research team did was they got their hands on what's called an …….

7 They…… many, many successful ……..

8 And they were able to change therapies, including disabling the device -- and this is with a real, commercial, …… device -- simply by performing reverse engineering and sending …… signals to it.

9 Now, wireless and the Internet can …….. health care greatly.

10 Okay, let me shift ……. and show you another ……

3. Watch the second part of the video again. Each of these sentences contains ONE mistake – find the mistakes and correct them.

1 This is a car, and it has a lot of components, a lot of electronics in it today. In fact, it's got many, many different computers inside of it, more Macs than my lab did when I was in college, and they're connected by a wireless network.

2 One is long-range wireless, where you can actually communicate with the device from nearby, either through Bluetooth or wi-fi, and the other is long-range, where you can talk with the car through the cellular network, or through one of the radio stations.

3 The second threat model was to see what someone could do if an attacker actually got access to the internal network on the car.

4 They put a PC, and they connected to the diagnostic unit on the in-car network, and they did all kinds of clever things, like here's a picture of the speedometer showing 140 miles an hour when the car's in park.

5 They also were able to install software that wouldn't kick in and wouldn't trigger until the car was doing something like going over 40 miles an hour, or something like that.

6 What you see here in number two is a reflection in somebody's glasses of the telephone that they're typing in.

7 There's one little point that shows up on the screen, and one little tiny turn of the switch.

8 The last one I thought was really, really cool, and I just had to show it to you, it's probably not something that you're going to lose sleep out like the cars or the defibrillators, but it's stealing key.

4. Ask your partners these questions:

1 How would you have reacted to the facts in this video?

2 What are some more disadvantages of other devices from the point of view of security threats?

3 Have you ever faced any security threats?

4 How to protect yourself from being hacked?

5 What advice could you give?

Reading

1B. Cyber Threats to Mobile Phones

Vocabulary

capability n. – техническая возможность

purse n. – кошелек

lax – слабый, небрежный

attractive adj. – привлекательный

outsell v. – превосходить по уровню/объему продаж

distribute v. – распространять

sophistication n. – сложность

countermeasure n – контрмера

catch up v. – наверстать

shortcoming n. – недостаток, изъян

surfing the internet – бродить по Интернету

wealth n. – изобилие

conduct v. – проводить

redeem coupon – отоваривать купон

point-of-sale payments – платежи через терминал

jeopardize v. – подвергать опасности

counterpart n.–аналогичный компонент

1. You are going to read the article about cyber threats to mobile phones. Three paragraphs have been removed from the article. Choose from the paragraphs A-C the one which fits each gap (1-3).

Smartphones, or mobile phones with advanced capabilities like those of personal computers (PCs), are appearing in more people's pockets, purses, and briefcases. Smartphones' popularity and relatively lax security have made them attractive targets for attackers. According to a report published earlier this year, smartphones recently outsold PCs for the first time, and attackers have been exploiting this expanding market by using old techniques along with new ones. One example is this year's Valentine's Day attack, in which attackers distributed a mobile picture-sharing application that secretly sent premium-rate text messages from the user's mobile phone. One study found that, from 2009 to 2010, the number of new vulnerabilities in mobile operating systems jumped 42 percent. The number and sophistication of attacks on mobile phones is increasing, and countermeasures are slow to catch up.

1

Unfortunately, many smartphone users do not recognize these security shortcomings. Many users fail to enable the security software that comes with their phones, and they believe that surfing the internet on their phones is as safe as or safer than surfing on their computers.

Meanwhile, mobile phones are becoming more and more valuable as targets for attack. People are using smartphones for an increasing number of activities and often store sensitive data, such as email, calendars, contact information, and passwords, on the devices. Mobile applications for social networking keep a wealth of personal information. Recent innovations in mobile commerce have enabled users to conduct many transactions from their smartphone, such as purchasing goods and applications over wireless networks, redeeming coupons and tickets, banking, processing point-of-sale payments, and even paying at cash registers.

2

Losing a mobile phone used to mean only the loss of contact information, call histories, text messages, and perhaps photos. However, in more recent years, losing a smartphone can also jeopardize financial information stored on the device in banking and payment apps, as well as usernames and passwords used to access apps and online services. If the phone is stolen, attackers could use this information to access the user's bank account or credit card account. An attacker could also steal, publicly reveal, or sell any personal information extracted from the device, including the user's information, information about contacts, and GPS locations. Even if the victim recovers the device, he or she may receive many spam emails and SMS/MMS messages and may become the target for future phishing attacks.

3

A. Some personal and business services add a layer of authentication by calling a user's mobile phone or sending an additional password via SMS before allowing the user to log onto the service's website. A stolen mobile phone gets an attacker one step closer to accessing the services as the user. If the device contains the owner's username and password for the service, the attacker would have everything necessary to access the service.

B. Smartphones and personal digital assistants (PDAs) give users mobile access to email, the internet, GPS navigation, and many other applications. However, smartphone security has not kept pace with traditional computer security. Technical security measures, such as firewalls, antivirus, and encryption, are uncommon on mobile phones, and mobile phone operating systems are not updated as frequently as those on personal computers. Mobile social networking applications sometimes lack the detailed privacy controls of their PC counterparts.

C. Many users may consider mobile phone security to be less important than the security of their PCs, but the consequences of attacks on mobile phones can be just as severe. Malicious software can make a mobile phone a member of a network of devices that can be controlled by an attacker (a "botnet"). Malicious software can also send device information to attackers and perform other harmful commands. Mobile phones can also spread viruses to PCs that they are connected to.

Writing

Write the description of one of the typical cyber attack and steps to protect your mobile phone from it. When you have finished, compare your description with your partner's.

Case Study: Espionage Campaign against the UK Energy Sector

Study this situation and then discuss the questions below.

Attackers used a technique known as a 'watering hole' attack to distribute malware into businesses working in the UK energy sector. The attackers added scripts to legitimate websites frequented by energy sector staff. Many of the websites were managed by the same web design company. Visitors' browsers were automatically and surreptitiously redirected to download malware from an attacker-owned server.

The malware targeted known and patchable vulnerabilities in Java, older internet browsers, and all but the most recent versions of Microsoft Windows. The malware harvested visitors' credentials and computer system information, and sent this information back to the controllers via attacker-owned domains.

How it happened: the technical details

In the survey stage, the attackers discovered that a single web design company hosted a number of energy sector businesses' websites. Although we can't say for sure how the attacker delivered the attack to breach the site, they may have infiltrated the web design company's networks by masquerading as a legitimate user with credentials stolen through successful spear-phishing, or by exploiting an unpatched vulnerability on the web server.

The attacker compromised the web server and then added code which caused their own website to be loaded whenever the legitimate website was visited. The delivery stage then involved the attacker's website delivering the malicious code to the victims' computers. The unpatched browsers were breached through known software flaws in Java and common internet browsers.

The attacker's website installed a Remote Access Tool (RAT) on the visitor's computer, disguised as a common type of web application script. The malware then started communicating with the attacker-owned domains by sending 'beacons' to show it was active and to request commands from the attackers. The malware was designed to capture system information, user

keystrokes and clipboard contents to enable the attackers to consolidate their position as they moved towards affecting their target. However, security monitoring of network activity detected command and control messages from malware on the infected computers, and in this case the attack was broken before it could affect the targeted businesses.

Survey ⟶ **Delivery** ⟶ **Breach** ⟶ **Affect**

Definitely these 'watering hole' attacks were part of a continuing espionage campaign against the UK energy sector.

What techniques did the attackers use to compromise their targets within the energy sector?

What are the most effective mitigations against this attack (both at the website and within the victim organization)?

Grammar: Gerund-Infinitive

1. Fill in the corresponding form of the infinitive.

1 he left to have left
2 he is playing……..
3 he will be expelled……..
4 he has called…….
5 he is advised……
6 he has been driving……
7 he was practicing…….
8 he swims…….
9 he will be skating……
10 he has been promoted……..

2. Put the following verbs into the correct category.

verb + to-inf	
verb + bare inf	
verb + -ing form	

avoid, regret, decide, want, promise, miss, hope, agree, mind, consider, finish, fancy, enjoy, deny, detest, refuse, let sb, should, expect, resist, can't stand, can, claim, make sb.

3. Put the verbs in brackets into the correct form of the infinitive or –ing form.

1 John was unable …… (play) computer games as he was about …… (have) an operation on his eyes.
2 I'm sorry ……. (say) that his recent car accident has made it impossible for John ……. (qualify) for the position of IT manager in the big company.
3 "I've never seen such a fast virus in my life! It's worth ……. (protect) your device; it's sure ……. (destroy) it.
4 I would prefer ……. (go) to the football match instead of ……. (watch) it on TV last night.
5 I can't help …… (think) how good Julie is as a programmer. I think she ought ……. (take) it up professionally.
6 It's no use …… (try) to make her have the use of this program. She'll start …… (fail) every time.
7 He claims ……. (be) the best computer player in the world, but he's never won anything in his life!
8 He seems to …….. (train) hard these days.
9 Bob was looking forward to …… (exploit) his new antivirus program.

10 As John was going to enter the university he spent all his time …….. (practice) for the finals.

4. Complete the gap in each sentence with the correct form of the verb in brackets.

1 The Help facility enables users …… (get) advice on most problems.
2 Adding more memory lets your computer ……. (work) faster.
3 Windows allows you …… (display) two different folders at the same time.
4 The Shift key allows you ……(type) in upper case.
5 The MouseKeys feature enables you …….. (use) the numeric keypad to move the mouse pointer.
6 ALT+TAB allows you …… (switch) between programs.
7 The StickyKeys feature helps disabled people ……..(operate) two keys simultaneously.
8 ALT+PRINT SCREEN lets you ……. (copy) an image of an active window to the Clipboard.

5. Read the following sets of sentences and explain how the verbs in bold differ in meaning.

1 a) Don't **forget** to wear protective gear when climbing.
b) I'll never **forget** seeing the figure skating championship last year.
2 a) Did you **remember** to tell Chris to bring his laptop with him? We're going to work after rest.
b) I don't **remember** seeing John at school. Perhaps he was ill.
3 a) I **regret** to inform you that your exam fail will prevent you from entering this university.
b) He **regrets** hacking this site as it resulted in his big sentence.

4 a) The user had to **stop** to charge a mobile phone.

b) You should **stop** playing computer games if you want to work in this company.

5 a) If it's OK by you, I'd **prefer** to send your additional password via SMS on Monday rather than on Sunday.

b) I **prefer** changing passwords to any kinds of antiviruses.

6 a) I **hate** to tell you this, but they' re not punishing the attacker.

b) I **hate** working on the laptop when it's lagging.

7 a) He should **try** to conduct some transactions from his smartphone; he's doing his business remotely.

b) If she **tries** using the better application, her work might be easier.

Reading

1C. Security Threats on Cloud Computing

Vocabulary

utilize v. – использовать

exchange v. – обмениваться

collaboration tools – инструмент обеспечения совместных работ

backup v. – копировать

cash flow – движение наличных средств

convenience n. – удобство

issue n. – проблема, трудность

vulnerable adj. – уязвимый

employ v. – использовать

on-demand adj. – запрашиваемый

abuse v. – нарушать режим эксплуатации

forceful adj. – принудительный

brute-forcing –грубый метод

launch v.- запускать

integrity n. – целостность

internal adj. – внутренний

employee n. – сотрудник

external adj – внешний

session hijacking – перехват сеанса

eavesdropping n. – несекционное извлечение информации

harass v. – нападать

data breach – уязвимость данных

1. You are going to read the article about security threats on cloud computing. For sentences 1-6, choose the continuation (A, B or C) which you think fits best according to the text.

Cloud computing has been involved in everyone's life. It delivers applications and storage spaces as services over the Internet for little to no cost. Most of us utilize cloud computing services on a daily basis. For example, we use web-based email systems (e.g. Yahoo and Google) to exchange messages with others; social networking sites (e.g. Facebook, LinkedIn, MySpace, and Twitter) to share information and stay in contact with friends; on-demand subscription services (e.g. Netflix and Hulu) to watch TV shows and movies; cloud storages (e.g. Humyo, ZumoDrive, and Dropbox) to store music, videos, photos and documents online; collaboration tools (e.g. Google docs) to work with people on the same document in real time; and online backup tools (e.g. JungleDisk, Carbonite, and Mozy) to automatically back up our data to cloud servers. Cloud computing has also been involved in businesses; companies rent services from cloud computing service providers to reduce operational costs and improve cash flow.

There is no doubt that the convenience and low cost of cloud computing services have changed our daily lives; however, the security issues associated with cloud computing make us vulnerable to cybercrimes that happen every day. Hackers employ a variety of techniques to gain access to clouds without legal

authorization or disrupt services on clouds in order to achieve specific objectives. Hackers could trick a cloud into treating their illegal activity as a valid instance, therefore, gaining unauthorized access to the information stored in the cloud.

Cloud computing involves delivering computing resources (e.g. servers, storages, and applications) as services to end users by cloud computing service providers. End users access on-demand cloud services through web browsers. Cloud computing service providers offer specific cloud services and ensure the quality of the services. Basically, cloud computing includes three layers: the system layer (Infrastructure-as-a-service (IaaS)), the platform layer (Platform-as-a-Service (PaaS)), and the application layer (Software-as-a-Service (SaaS)).

Three cloud service models (SaaS, PaaS and IaaS) not only provide different types of services to end users but also disclose information security issues and risks of cloud computing systems. First, the hackers might abuse the forceful computing capability provided by clouds by conducting illegal activities. IaaS is located in the bottom layer, which directly provides the most powerful functionality of an entire cloud. It maximizes extensibility for users to customize a "realistic" environment that includes virtual machines running with different operating systems. Hackers could rent the virtual machines, analyze their configurations, find their vulnerabilities, and attack other customers' virtual machines within the same cloud. IaaS also enables hackers to perform attacks, e.g. brute-forcing cracking, that need high computing power. Since IaaS supports multiple virtual machines, it provides an ideal platform for hackers to launch attacks (e.g. distributed denial of service (DDoS) attacks) that require a large number of attacking instances.

Second, data loss is an important security risk of cloud models. In SaaS cloud models, companies use applications to process business data and store customers' data in the data centers. In PaaS cloud models, developers use data to test software integrity during the system development life cycle (SDLC). In IaaS cloud models, users create new drives on virtual machines and store data on

those drives. However, data in all three cloud models can be accessed by unauthorized internalemployees, as well as external hackers. The internal employees are able to access data intentionally or accidently. The external hackers gain access to databases in cloud environments using a range of hacking techniques such as session hijacking and network channel eavesdropping.

Third, traditional network attack strategies can be applied to harass three layers of cloud systems. For example, web browser attacks are used to exploit the authentication, authorization, and accounting vulnerabilities of cloud systems. Malicious programs (e.g. virus and Trojan) can be uploaded to cloud systems and can cause damage. Malicious operations (e.g. metadata spoofing attacks) can be embedded in a normal command, passed to clouds, and executed as valid instances. In IaaS, the hypervisor (e.g. VMware vSphere and Xen) conducting administrative operations of virtual instances can be compromised by zero day attack.

It is necessary to identify the possible cloud threats in order to implement better security mechanisms to protect cloud computing environments. In the following subsections, we explored security threats presented in clouds from three perspectives: abuse use of cloud computational resources, data breaches, and cloud security attacks. Recent real world cloud attacks were also included to demonstrate the techniques that hackers used in exploiting the vulnerabilities of cloud systems.

1Hackers employ a variety of techniques

A. to steal data legally

B. to get access to clouds without legal authorization

C. to offer specific cloud services

2 Cloud computing includes

A. 4 layers

B. 2 layers

C. 3 layers

3 IaaS is located in

A. the bottom layer

B. the platform layer

C. the application layer

4 The external hackers gain access to databases in cloud computing such as

A. changing passwords

B. session hijacking

C. brute-forcing cracking

5 Malicious programs can be uploaded to cloud systems and can cause

A. damage

B. change

C. launch

6 In IaaS the hypervisor can be compromised by

A. cracking

B. session hijacking

C. zero day attack

Writing

1. Look at the list of instructions how to write a summary/abstract. Put them into the right order.

- Work out a logical sequence for the listed words.
- Make a list of these points in your own words.
- Write the summary linking the key points together using connecting and/or reference words.
- Write the final draft.
- Underline the important points/ sub points.
- Read and understand the text. Try to understand the main purpose of the author (message). It is often pointed out in the title or introductory sentence.

Check your first draft, paraphrase the words of the article as much as possible.

2. Summarize the information of the article according to the following points and write the summary/abstract:
    - introduction (what is cloud computering)
    - cloud service models
    - taxonomy of cloud security threats
    - conclusion

Role-play

Participants:

Speaker

Reporter

Judge

Work in groups of three, A, B and C.

Play the roles in rotation: Speaker, Reporter and Judge.

The Speaker explains the main points of one text (1A, 2A, 3A) using only the picture below.

The Reporter listens carefully and reports back to the Speaker a summary of the main points.

The Judge listens carefully to both Speaker and Reporter and points out any mistakes, main points omitted or additions the Reporter has made.

Repeat this activity until you have played all these roles and all of your texts have been covered.

Assignments for Self-Evaluation: Examination Paper Sample

<u>Vocabulary Test</u>

Complete the passage with the best option from the list below.

<u>New Bluetooth Hack Affects Millions of Devices from Major Vendors</u>

Yet another bluetooth hacking technique has been uncovered. A highly critical 1_____has been found affecting some Bluetooth implementations that could allow an 2_____, remote attacker in physical proximity of targeted devices to intercept, monitor or manipulate the traffic they exchange. The Bluetooth hacking vulnerability, tracked as CVE-2018-5383, affects firmware or 3_____from some major vendors including Apple, Broadcom, Intel, and Qualcomm, while the implication of the 4_____on Google, Android and Linux are still unknown.

The security 5_____is related to two Bluetooth features—Bluetooth low energy (LE) implementations of Secure Connections Pairing in operating system software, and BR/EDR implementations of Secure Simple Pairing in device firmware.

Researchers from the Israel Institute of Technology discovered that the Bluetooth specification recommends, but does not mandate devices supporting the two features to validate the 6_____received over-the-air during secure pairing.

Since this 7_____is optional, some vendors' Bluetooth products supporting the two features do not sufficiently validate elliptic curve parameters used to generate 8_____during the Diffie-Hellman key exchange.

In this case, an unauthenticated, remote attacker within the range of 9_____during the pairing process can launch a man-in-the-middle attack to obtain the cryptographic key used by the device, allowing them to potentially snoop on supposedly encrypted device communication to steal data going over-the-air, and 10_____.

Here's what the Bluetooth Special Interest Group (SIG), the maintainers of the technology, says about the flaw:

"For an attack to be successful, an attacking device would need to be within wireless range of two 11_____Bluetooth devices that were going through a pairing procedure."

"The attacking device would need to intercept the public key exchange by blocking each transmission, sending an acknowledgment to the sending device, and then injecting the malicious packet to the receiving device within a narrow time window. If only one device had the 12_____, the attack would not be successful."

1.	a)	malware download	b)	cryptographic vulnerability	c)	bot
2.	a)	unauthenticated	b)	unnoticed	c)	corrupted
3.	a)	malware download	b)	operating system software drivers	c)	hardware
4.	a)	criminal	b)	hacker	c)	bug
5.	a)	data breaches	b)	personal losses	c)	vulnerability
6.	a)	public encryption key	b)	cryptographic vulnerability	c)	steganography
7.	a)	specification	b)	prolongation	c)	target
8.	a)	home keys	b)	instruments	c)	public keys
9.	a)	compromised devices	b)	closed devices	c)	targeted devices
10.	a)	inject malware	b)	kill somebody	c)	impact a vendor
11.	a)	attacked	b)	encrypted	c)	vulnerable
12.	a)	availability	b)	vulnerability	c)	encryption

Grammar

Choose the correct option.

1. This is the subject about ……we don't know much.
   a. what b. whose c. which

2. Generally, a new computer …….. a few thousand calculations in a few seconds.

a. is carrying b. carries c. carrying

3. If I …….you, I would recheck the results of our experiment.
   a. were b. am c. will be

4. These tools constantly need …….. updated if they have a chance of being effective.
   a. be b. being c. to be

5. We …… see electrical devices everywhere.
   a. should to b. must c. can

6. Hard drive has a ……. capacity than other devices.
   a. more larger b. more large c. larger

7. Cache memory…….. faster than RAM.
   a. is b. are c. be

8. They ……..this project yet.
   a. haven't finished b. didn't finished c. have finished

9. The ……. industry produces several types of minicomputers.
   a. electricity b. electronic c. electrical

10. When …… monitoring we are typically watching specific items of data we have collected.

a. conducting b. conduct c. doing conduct

READING COMPREHENSION

Read the text and answer the questions below

Nowadays computers, smartphones, and tablets – all smart devices – dominate our daily lives. We rely heavily on these devices for our work and business needs, as well as for our social, and dating lives. However, this dependence on technology can also make us vulnerable.

Is something sinister occurring when you use your computer or is it merely not operating to its full potential? Perhaps your smartphone or tablet is also acting up. Viruses are incredibly common and can affect more than just your PC. Let's uncover the key signs that you have been hacked.

Getting Redirected

Viruses commonly redirect your web browser to certain sites. This is generally an attempt to get you to pay money for a product or service on these web pages. So, if you keep finding yourself on sites you never searched for, then something is up.

First, make sure it is not the web page you are on that is doing the redirecting. Visit familiar websites that you know will not redirect you. Next, consider that a poorly set-up browser can also cause these issues. Try using a different browser for a while to find out. If you have established that neither of these is the case, then it is time to consider that you have been hacked by a virus.

Another related issue is that your homepage may have been changed without your knowledge. Although viruses can commonly do this, legitimate software may also be the culprit. When installing a new program, there is often a check box asking for permission to change your browser settings or homepage, which people often rush past without unchecking. Try changing your homepage back to normal, and if it keeps reverting to the unwanted site, then you may have a malware infection.

Pop-up Bombardment

These pesky ads are a common occurrence when visiting certain websites. However, particular viruses can bombard you with these pop-ups, even when you are not using your web browser.

If your interface is being overloaded with pop-up boxes even when you are not surfing the web, then there is likely something wrong. Run a virus scan to determine the culprit and eliminate these annoying ads.

Snail-like Speeds

If you are experiencing very slow operating speeds, this is another indication of potential virus activity. First, make sure it is not caused by a resource heavy program operating in the background. Also check that your hard drive isn't running out of space, or that you have insufficient RAM for your day-to-day tasks. If you have assessed these factors and still believe your computer or device is running slowly for an unknown reason, then it could be a malware infection.

Ghost Messages

If you are seeing messages to your friends that you do not remember sending, then something is amiss. This often happens with email but could also occur through Facebook, Skype, or other communication platforms. The messages will often have a link attached in the hope that readers will click on it. The link will get directed to a site that might infect their computer, or encourage them to purchase something. They may also contain attachments that download malware directly to the person's computer or device.

The first step you should take is letting the recipients of these messages know that they are not from you, and not to open them or click on any attachments/links included in the message. Afterward, it is time to run some quality anti-virus software so that your phantom messages do not cause any more drama for others.

Trojan Treachery

Perhaps you have recently installed some antivirus software that may not be from the most reputable or well-researched location. Certain programs will run scans telling you that your system is overrun with thousands of infections, and then inform you that the only way to remove them is to upgrade to the full version. This version typically carries a heavy price tag.

These programs are known as Trojans. They appear to be helpful but are viruses themselves. Diligently research before downloading any antivirus software – or any software in general – to prevent trojans from inhabiting your system.

Fighting Back

If you have experienced any of these signs and are concerned about the integrity of your system, do not wait. It's important to create a smart lock on your computer. A strong firewall should be set up with regular scans and quality anti-malware software should be undertaken. Also, practice due diligence when opening strange email attachments, links, and downloading files you are unfamiliar with.

Taking these precautions grant security for your computer and other electronic devices. You will be able to work, play on social media, shop online, and more without constantly being under the looming shadow of a computer virus.

1) What dominates our daily lives these days?
2) What can make us vulnerable?
3) Will you list the key signs showing that you have been hacked?
4) What do viruses commonly do?
5) What is the main goal of the virus?
6) What can a poorly set-up browser cause?
7) How can you understand that you have been hacked by a virus?
8) What do people often rush past without unchecking?
9) What are the signs that you have a malware infection?
10) What can happen to your computer when you visit certain unknown websites?
11) What indication is it if you are experiencing very slow operating speeds?
12) What can cause very slow operating speeds?
13) What is a ghost message?
14) What steps should you take if ghost messages were sent from your account?
15) What programs are known as Trojans?
16) What should you do to prevent Trojans from inhabiting your system?

17) What should be set up and what is important to create on your computer?
18) What precautions should be taken to protect your computer?

Speaking

Speak on one of the following topics. You should speak for 3-5 minutes. You have 10 minutes to prepare your speech.

1. Cybercrimes
2. Means of attack in cybercrime
3. Antivirus software

Unit 17 Standards and Specifications in the field of Information Security

Warm up

1. Decide in groups what these kinds of individuals who have involved into threats and attacks are. Then match the terms to the short descriptions which follow.

1 Black hat

2 Cracker

3 White hat

4 Hacker

5 Spammer

6 Phreaker

7 Phisher

A This is a general term that has historically been used to describe a computer programming expert. More recently, this term is commonly used in a negative way to describe an individual who attempts to gain unauthorized access to network resources with malicious intent.

B The term that is generally regarded as the more accurate word that is used to describe an individual who attempts to gain unauthorized access to network resources with malicious intent.

C An individual who manipulates the phone network to cause it to perform a function that is normally not allowed. A common goal of this is breaking into the phone network, usually through a payphone, to make free long-distance calls.

D An individual who sends large numbers of unsolicited e-mail messages. They often use viruses to take control of home computers to use these computers to send out their bulk messages.

E An individual uses e-mail or other means in an attempt to trick others into providing sensitive information, such as credit card numbers or passwords. The phisher masquerades as a trusted party that would have a legitimate need for the sensitive information.

FA term used to describe individuals who use their abilities to find vulnerabilities in systems or networks and then report these vulnerabilities to the owners of the system so that they can be fixed.

G Another term for individuals who use their knowledge of computer systems to break into systems or networks that they are not authorized to use.

2. Look at the pictures which depict how a social engineer can operate. Try to answer these questions without reading the texts.

1 What is social engineering?
2 How do social engineers work?
3 Why is the title called “Hacking the Mind”?

3. Scan these texts to check your answers to Task 2. Could you give more examples of "hacking people"?

Reading

2A. Playing Well with Others: Human Interaction 101, "The Bump"

Vocabulary

regardless adv. – невзирая на

interact v. – взаимодействовать

engage v. – вовлекать

facility n. – возможность

interpersonal adj. – межличностный

emerge v. – выходить

rapport n. – отношение, взаимопонимание

entire adj. – полный

likelihood n. - вероятность

pop v. – внезапно появляться

explicitly adv. – однозначно

determine v. – определяться

stunning adj. – потрясающий

sash n. – шарф

beany n. –круглая шапочка с полями

tempting adj. – соблазнительный, искусительный

utter v. – произносить

shove v.- швырять

eavesdrop v.– перехватывать информацию

congruence adj. – совпадающий

creepy adj. –отвратительный

stalker n. – упорный преследователь

shield n. – защита, щит

self-awareness n. – самосознание

compliance n. – согласие

chit chat – болтовня

mindful adj. – внимательный

respectful adj. – уважительный

albeit adv. – пусть и

time constrain – ограничение во времени

in a nutshell–в двух словах, короче говоря

1. You are going to read the article about human interaction in social engineering. Choose from the list A-D the question which best matches each part (1-4) of the article.

A Are you a threat?
B How much time is this going to take?
C Who are you?
D What do you want?

Are you a social engineer? Regardless of your profession, the answer is yes! Because we are social creatures living and interacting with others, chances are that you will engage in a number of activities that in one way or another facilitates your existence within human society. Even those of us who prefer the relative interpersonal safety of online interactions will, at some point, emerge to buy a cup of coffee (or horrors!) say hello to the neighbor.

The approach, or "bump" in the development of rapport with an individual is very important. How well (or poorly) you execute this can set the tone for the entire interaction, and ultimately, determine its success.

Think about the last time you were approached by a stranger. In all likelihood, a number of questions popped immediately into your head:Who is this person? Are they a threat? What do they want? How much time is this going to take?

If the stranger was able to answer these questions, you probably allowed the interaction to proceed. These questions don't have to be answered explicitly, but if they're not addressed to a level of comfort determined by the target, chances of getting one's way get pretty slim.

An example of a group who answers ALL of these questions to stunning effect are those little girls you're probably seeing sitting at tables right now

inside your local supermarket. With their sashes, beanies, bright smiles and tempting displays, they answer all of those questions without uttering a single word. In fact, the last time I was approached by one of these demon children I found myself shoving money at her before she even opened her mouth.

Whether in the context of a social engineering engagement or an everyday interaction, the key here is that there is generally a purpose – it could be as simple as getting to know someone, all the way up to and including attempting to influence a decision. But you're never going to reach that point until you answer those four questions in the mind of your target.

1

It's a simple enough question. The answer doesn't have to be a mechanical, "Hello, I am Doug, your friendly technical support person." Who you are is communicated in all kinds of ways without you ever saying a word. We people-watch (and more often in the age of technology, eavesdrop) all the time, and often come to conclusions about who we observe. Are they married? Educated? Nice or mean? In a social engineering engagement, the keys are congruence and playing to stereotypes, as painful as that may be. Everything about you (attitude, appearance, language, etc.) should confirm your pretext, and most importantly, not cause any additional questions in the mind of the target.

2

This is really a sub-question under "Who are you?" If the answer is, "I'm a creepystalker," then you've pretty much answered this question as well. This is reasonable for anyone to ask, and one that you as a social engineer must address immediately. You can't develop rapport if your target has their shields up. This requires some self-awareness on your part. What messages do you communicate non-verbally? Again, this goes back to congruence. If you're trying to act in a friendly fashion but your face or body conveys something else, your target will notice….something. That something may be enough reason to shut you down.

We once had a young lady take our test. She was a delightful and engaging individual, so we were a bit mystified when she reported some difficulties with her "bumps" during homework. What we eventually discovered was that whenever she was nervous or thinking intently, she made what appeared to be a very angry face, which was making her targets uneasy. Once she became aware of this tendency, she was able to change it and experienced great success in both her approach and rapport-building.

Humans are generally excellent at detecting what appears to be anger or aggression, for obvious and adaptive reasons.

3

You're asking for something, whether that's basic information or compliance. But the true nature of the question has more to do with the level of the request. In other words, someone you just met will probably not agree to help move you and your family across country. But they may be willing to engage in some light chit chat, provided you answered questions 1 and 2 above. The level of request should be consistent with the level of relationship you have established at that point. So in the chit chat scenario if you continue to ask personal questions of your target without offering anything in return (which starts to feel less like a relationship and more like a creepy interrogation), you'll rapidly exceed what's appropriate and comfortable for the target.

4

Most of us have places to go and things to do. So letting the target know you are mindful and respectful of their time makes it much easier and less risky to engage with you. It provides structure (albeit usually artificial) to the situation, which will also increase comfort. We often talk about the artificial time constraint as an invaluable tool in the development of quick rapport. This is another one of those questions that doesn't have to be answered explicitly. There

are lots of ways to indicate that you don't plan on monopolizing your target all day.

So you now have all you need to know about making a "bump", which is the gateway to building rapport and creating influence. In a nutshell, it's all about making your target feel as comfortable as possible by taking any sort of risk you pose out of the situation.

2. Read the article again and do the following task. For sentences 1-6, choose the continuation (A, B or C) which you think fits best according to the text.

1 According to the text, you are a social engineer

A regardless of your age

B regardless of your profession

C regardless of your gender

2 The author is under impression that a number of questions popped into your head are

A 4

B 6

C 8

3 In a social engineering engagement, the keys are

A different

B incongruence

C congruence

4If you are trying to act in a friendly fashion but your face or body conveys something else

A you'll fail

B the target won't notice anything

C you'll succeed

5 The true nature of the question has

A a creepy interrogation

B more to do with the level of the request

C personal relationship

6 We often talk about the artificial time constraint as a tool in the development of

A contact

B rapport

C impression

3. Match the words. Make sentences using them.

A	B
time	safety
chit	interaction
interpersonal	effect
local	display
stunning	supermarket
communicate	money
creepy	engineering
social	non-verbally
shove	chat
entire	constraint

Language Focus

1. How much do you know about cyberspace? Work with a classmate to match the word with its definition. Then change the word form in the e-mail below if necessary.

1 emoticon
2 instant messaging (IM)
3 chat
4 spam
5 surf
6 wireless

a junk e-mail; e-mail you don't want from someone you don't know
b real-time communication in writing between two people
c use the Internet to look for information
d a symbol for feelings
e Internet connection without a cable
f real-time communication in writing among more than two people

2 Use the words from Task 1 to fill in the blanks of the e-mail.

Hi, Carlos,

I was watching TV last night with my computer on my lap – like I always do/ while I was 1 _____the Web, my neighbor knocked on the door. She wanted me to teach her how to use 2_____. She wanted to be able to "talk" with her daughter in Connecticut. You know I have a high-speed 3_____ connection, so I use IM quite a lot. I showed her how to add her daughter to her e-mail contacts and how to start up her IM Program. I even showed her how to send a message with a couple of

4_____. I showed her the smiley face one: ☺. Of course, she wasn't happy with only that. She said she also wanted to be able to 5_____with a lot of people at the same time, so I had to show her how to enter a chat room. She still wasn't finished, though! She asked me how to stop getting e-mail she wasn't interested in, so I showed her my program to stop 6_____and told her where she could buy it/ she said she'd be back tonight so I could help her install it on her laptop. That's why I'm writing you from an Internet café tonight!

See you soon!

Jim

3 Study the verbs below. Then, circle the correct verb to complete each sentence.

convince v. to make someone believe in something
emerge v. to appear, to begin
expand v. to grow bigger
overwhelm v. to present with an excessive amount
persist v. to hold firmly to a purpose
persuade v. to make someone do something
scroll v. to move up and down a computer screen

1. I_____ in learning how to make a Web page and was finally successful.
   a. persuaded
   b. persisted
2. I'm _____with work this week. Can we have lunch next week instead?

a. overwhelmed
b. urged

3. Joan, can you _____ your boyfriend to help me install an anti-virus program? I get a lot of junk e-mail, and I'm afraid I'll get a computer virus.
   a. scroll
   b. persuade
4. I'm _____that I need to get a new Internet Service Provider (ISP). What do you think?
   a. convinced
   b. expanded
5. He _____ me to stop sending him e-mail to his office account. He said that his boss might see it and wouldn't like it.
   a. urged
   b. emerged

Listening

Hackers: the Internet's Immune System

1. You'll watch the video. Try to catch the general idea.
2. Watch the video again. Fill each gap in this summary with ONE only.

1. Four years ago, a …….. researcher, or, as most people would call it, a hacker, found a way to literally make ATMs throw money at him.
2. Barnaby Jack could have easily turned into a career …….. or James Bond villain with his knowledge, but he chose to show the world his research …….
3. Sometimes they make us sick, but they also find those …….threats in our world, and they make us …… it.

4. I was such a ……. back then that even the boys on the Dungeons and Dragons team wouldn't let me join.
5. It was a simple ……., and I was just a script kiddie back then, but to me, that trick, it felt like this, like I had discovered …….. potential at my fingertips.
6. But what if you could read your ex's emails, or add a couple …….. to your bank account.
7. This is what happened last year when another security researcher called Kyle Lovett discovered a gaping …… in the design of certain wireless routers like you might have in your ……. or office
8. He reported it to the company, of course, but they ignored his ……..
9. Making …… known to the public is a practice called full disclosure in the hacker community, and it is controversial, but it does make me think of how …….. have an evolving effect on technologies we use every day.
10. Thankfully for Khalil, a group of hackers were watching out for him. In fact, they raised more than …….. dollars to reward him for this discovery, raising a …… discussion in the technology industry about how we come up with incentives for hackers to do the right thing.
11. These are things that will come ……. and bite you.
12. I find it astounding that someone from the shadowy corners of …….. can become its voice of opposition, its last line of …… even, perhaps someone like Anonymous, the leading brand of global hacktivism.
13. This is when Anonymous was forged out of the seemingly ……. collection of Internet dwellers.
14. The reality is, hackers can do a lot more than …….. things.
15. They found European service providers that still had ……-year-old analog dial-up …….. infrastructure.

16. This tweet was …….., of course, but the resulting …….. in the Dow Jones index that day was most certainly not, and a lot of people lost a lot of money.
17. They come from all walks of ……, ethnicities, ideologies and genders, I might add.
18. He's the NSA director and U.S. ……. commander, but instead of his four star general uniform, he was wearing …… and a t-shirt.
19. My years in the hacker world have made me realize both the problem and the ……..about hackers.
20. They make us, they force us to fix things or demand something better, and I think we need them to do just that, because after all, it is not information that wants to be ……, it's us.

3. Watch the video again. Each of these sentences contains ONE mistake – find the mistakes and correct them.

1 I'm here today because I think we really need hackers.

2 He believed that sometimes you have to demo a threat to spark a decision.

3 So I am here today because I think we need hackers, and in fact, they just might be the immune system for the Stone Age

4 I knew that I might get hacked for giving this communication, so let me save you the effort.

5 He learned that anyone could remotely connect to these devices over the Internet and download documents from soft drives attached to those routers, no password needed.

6 By getting into people's files like that, yeah, they broke the law, but they also forced that company to break their product.

7 It is even more false if we go after hackers that are willing to risk their own freedom for ideals like the freedom of the web, especially in times like this, like today even, as governments and corporates fight to control the Internet.

8 This type of thing is happening all over the world right now.

4. Make up five questions according to the video and discuss them in groups.

Reading

2B. Don't make THAT face!

Vocabulary

percentage n. – процентное соотношение

statement n. – утверждение

nonverbally adv. – относящийся к неречевой информации

field n. – область

prematurely adv. – преждевременно, досрочно

engagement n. – назначенная встреча

oxytocin n. – окситоцин

bloodstream n. – кровообращение

appropriate adj. – соответствующий

validation n. – подтверждение

dopamine n. – дофамин

ventral adj. – передний

tilt n. – наклон

leakage n. – утечка

deep-seated adj. – укоренившийся

fascinating adj. – очаровательный

elicit v. – вызывать

furrowed brow– наморщенный лоб

pursed lips– сморщенные губы

budding adj. – перспективный

stimuli n. – руководство к де йствию

embrace v. - применять

conscious adj. – осознанный, осмысленный

1. You are going to read the article about mastering nonverbal SE by Chris Hadnagy. Eight sentences have been removed. Choose from the sentences (A-J) the one which fits each gap.

In my time and work with Dr. Ekman, I have learned to not put an exact percentage on this next statement, but some researchers claim that even up to 80% of what we say is nonverbally transmitted. 1-

2- The interesting part for me is that as important as nonverbal communication is to us as humans, our field of security tends to not focus on how seriously it can affect our work. The wrong nonverbal at the wrong time can send the…. wrong message. And if the wrong message is sent, we can prematurely end our engagements.

That feeling releases a chemical called oxytocin into the bloodstream. Trust opens the person up. When this release of oxytocin is followed up by the appropriate level of validation, it will release dopamine into the bloodstream. When this is done naturally and correctly, what is theresult? 3-

Now, how would you feel if you were doing a near–perfect job at trust building, rapport building, and validation, but when you expected to see this face:

you were instead met with this face:

4-

One of the reasons for this possible incongruence between what you think should happen and what actually happens your own nonverbal leakage. Nonverbal leakage is when your nerves, your own emotions, or your real beliefs about the target's beliefs or statements leaks out.

This is hard, if not impossible, to control, especially on topics on which you have a very deep–seated belief.

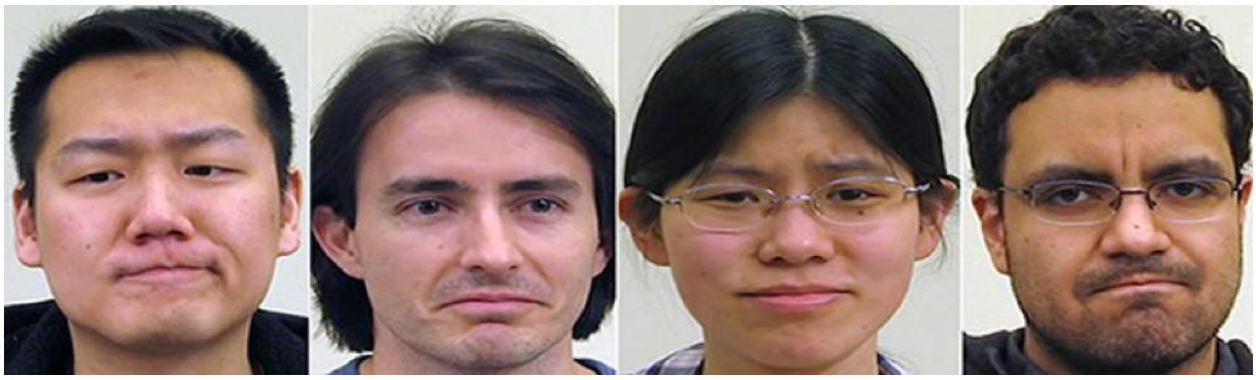
Enter the "NOT FACE"

5- their paper titled, "The not face: A grammaticalization of facial expressions of emotion" researchers Benitez-Quiroza, Wilburb, and Martinez found what they are calling a "universal expression" indicating disagreement.

In their test they covered major language and culture groups such as English, Chinese, Spanish, and American Sign Language. In each group they spoke to the person in their native language and asked them questions that would elicit a negative response. They took video recording their faces during the response, then cataloged which muscles moved when answering. All of this allowed them to make this claim of a finding a "not face."

6- The "not face" is characterized by a furrowed brow, pressed lips, and raised chin — all indicators of negative stressors. Pursed lips are indicative of stress, disagreement or anger. A raised chin is seen as contempt.

7- Some of the images they captured are below, and it is clear that none of the faces show agreement:



What does this mean for social engineers?

Understanding this is important for you and me since, if we know that we might be interacting with a target that has deep-seated beliefs that are opposing to ours, it would best to prepare ahead of time.

8- A few tips for the budding social engineers out there:

- Having your pretext planned out will help you prepare the emotional content you should display.
- Practice the nonverbal display your pretext would be showing.

- Role play before hand as part of your practice sessions.
- Don’t overthink it.
- Most importantly, since this is the way we are made, don’t try to consciously stop yourself from showing nonverbals. Instead, find a common ground, as common ground can help you display appropriate nonverbals.

In the end, you are a human (so I have heard), and humans display nonverbal expressions in response to external stimuli — you can’t stop that, besides using botox (which, by the way, I don’t suggest).Embrace your emotion, learn how to be more conscious while engaging, and think through your responses. All of these tips can help you become a master of what you display.

A From a nonverbal perspective, we can see it with open ventral displays of body language, natural head tilts, and smiling.

B Whether its 50, 60, or even 80% — we know it is A LOT.

C For example, we want to build rapport with our targets. Rapport is built by making the target feel you trust them.

DA team of researchers from Ohio State University recently got together to perform a study — and they found something quite fascinating.

E If you are like me, you would be pretty disappointed and even a little concerned.

F So how can you prepare?

G According to Dr. Paul Ekman and other facial expressions researchers, each of these have their place in other expressions, mainly negative: A furrowed brow in seen in anger as well as negative conversational signals.

H The researchers found that the subjects showed this sign of disagreement whether they were responding verbally in a negative fashion or thinking about the question asked negatively.

2. Look at the phrases taken from the article and explain the underlined parts in your own words.

1 When this release of oxytocin is followed up by the appropriate level of validation…

2 … what actually happens your own nonverbal leakage.

3 … especially on topics on which you have a very deep-seated belief.

4 Practice the nonverbal display your pretext would be showing.

5 Embrace your emotion, …

Writing

Write a news item like a short newspaper article about any hacking case known to you.

Case Study: How Hackers use Social Engineering

Study this situation and then discuss how this could be prevented.

In this case study, Ira Winkler, a professional social engineer, graciously shared an interesting study about how to hack with social engineering. This is a prime example of how not paying attention can get you hacked!

THE SITUATION

Mr. Winkler's client wanted a general gauge of the organization's security awareness level. Ira and his accomplice went for the pot of gold and tested the organization's susceptibility to social engineering.

To start, they scoped out the main entrance of the building and found that the reception area and security desk were in the middle of a large lobby and were staffed by a receptionist. The next day, the two men walked into the building during the morning rush while pretending to talk on cellphones. They stayed at least 15 feet from the attendant and ignored her as they walked by.

After they were inside the facility, they found a conference room to set up shop in. They sat down to plan the rest of the day and decided a facility badge would be a great start. Mr. Winkler called the main information number and asked for the office that makes the badges.

He was forwarded to the reception/security desk. Ira then pretended to be the CIO and told the person on the other end of the line that he wanted badges for a couple of subcontractors. The person responded, "Send the subcontractors down to the main lobby."

When Mr. Winkler and his accomplice arrived, a uniformed guard asked what they were working on, and they mentioned computers. The guard then asked them if they needed access to the computer room! Of course, they said, "That would help."

Within minutes, they both had badges with access to all office areas and the computer operations center. They went to the basement and used their badges to open the main computer room door. They walked in and were able to access a Windows server, load the user administration tool, add a new user to the domain, and make the user a member of the administrators' group. Then they quickly left.

The two men had access to the entire corporate network with administrative rights within two hours. They also used the badges to perform after-hours walkthroughs of the building. While doing so, they found the key to the CEO's office and planted a mock bug there.

THE OUTCOME

Nobody outside the team knew what the two men had done until they were told after the fact. After the employees were informed, the guard supervisor called Mr. Winkler and wanted to know who issued the badges. Mr. Winkler informed him that the fact that the security office didn't know who issued the badges was a problem in and of itself, and that he does not disclose that information.

Grammar: Conditionals-Wishes

1. Read the sentences and match them with the correct description. Then say what tense is used for each conditional sentence.
    1. If you heat water, it boils.
    2. If you hear the alarm, get onto the deck quickly.
    3. If I see someone trying to break in, I'll call the police.
    4. If I saw someone trying to break in, I would call the police.
    5. If I were you, I'd call the police.
    6. If I had seen someone trying to break in, I would have called the police.

    a. untrue condition in the present
    b. giving instructions
    c. imaginary situation contrary to the facts in the past
    d. general truth/scientific facts
    e. action likely to happen in the present/future
    f. giving advice

2. Fill in the correct tense then identify the type of conditional.

    1. If we lived in a well-built house, we_____(not/be) in danger.
    2. The car _____(not/roll) back as long as you put the brake on.
    3. You might cut yourself if you _____(play) with knives.
    4. I would always wear a helmet if I _____(be) you.
    5. If you'd locked the medicine up, he_____(not/drink).
    6. Supposing you _____(get) stuck in the lift, what will you do?
    7. If he_____ (listen) to the weather forecast, he wouldn't have sailed in such stormy weather.
    8. What _____ (you/do) if there was an emergency landing?
    9. If you hear the alarm,_____(head for) the exit.

10. If he had been driving more carefully, he_____(avoid) the accident.

3. Complete the following sentences.

1 If he had had a whistle, …he would have used it so that the rescue team could find him…

2 If the driver had seen the dog, _____

3 If you drive carefully,_____

4 Use the fire extinguisher_____

5 If you don't leave on time,_____

6 If you lose your way,_____

7 If there wasn't any fog,_____

8 If he hadn't lit a campfire,_____

9 If I were stuck on a deserted island, _____

10 if she hadn't drunk the water from the well, _____

4. Match the sentences with the meaning.

1. I wish they had discovered the bomb before it exploded.
2. I wish it would stop snowing.
3. I wish I had some food with me.

a. regret about a present situation we want to be different
b. wish for a future change unlikely to happen expressing disappointment
c. regret that something didn't happen in the past

5. Write wishes for the following situations.

1 Paul was driving carelessly and caused an accident.

…I wish Paul had been driving carefully…

2 Nina left her boots on the stairs and you tripped over them.

3 It has been snowing for hours and the rescue team cannot find the lost skiers.

4 You got a shock when you unplugged the heater with wet hands!

5 You are lost in the mountains and are unable to ask for help because your radio transmitter doesn't work.

6 You left the saucepan on the cooker and the oil caught fire.

7 You have a puncture and no spare tyre.

8 You are swimming and suddenly get a terrible cramp because you ate too much.

6. Complete the sentences using the words in the bold.

1 They didn't listen to the forecast and got trapped in the floods.

had If they_____ they wouldn't have got trapped in the floods.

2 If a fire breaks out, go to the nearest exit.

should Go to the nearest exit_____out.

3 It's a pity the fireman didn't rescue her.

had I wish _____her.

4 He got trapped in an avalanche while he was skiing.

gone If_____; he wouldn't have got trapped in an avalanche.

5 If I were a good swimmer, I could have saved him.

wish I_____a good swimmer; I could have saved him.

6 Unless you follow the path, you won't reach the cabin.

do If_____the path, you won't reach the cabin.

7 The authorities didn't act quickly, so the oil slick spread.

acted If _____quickly, the oil slick wouldn't have spread.

8 I didn't hear the warning so I didn't stay indoors.

wish I_____the warning; then I'd have stayed indoors.

9 It's that forests are destroyed by fires.

not I wish_____by fires.

10 The river flooded its banks, so our crops were ruined.

been If the river hadn't flooded its banks, our crops_____ruined.

Reading

2C. The Art of Deception

Vocabulary

script kiddies – взломщик-дилетант

bulletin board system – электронная доска объявлений

merely adv. – просто

happy-go-lucky adj. – беззаботный, шалопай

split v. – зд. уходить

harry v. – изводить

erratic adj. – изменчивый, непредсказуемый

youngster n. – юнец, парень

paper-punch n. – бумажный дырокол

transfer slip – передаточная ведомость

blank adj. – пустой, чистый

trash bin – урна

toss away - выбрасывать

shift n. – смена

pad n. – блокнот

surface v.- обнаруживаться

encounter n. – первый опыт, первое знакомство

employee n. - служащий

lingo n. – профессиональный жаргон

prank n. – зд. шуточный розыгрыш

dime n. – монета в 10 центов

pejorative n. – бранное слово

tinker v. – чинить кое-как, на скорую руку

suspension n. – приостановка

cum laude – с отличием

dread v. –с ужасом ждать

proverbial adj. – вошедший в поговорку, общеизвестный

salt mines – каторга

hone v. – затачивать, развивать

inherit v. – унаследовать

conartist–мошенник, аферист

swindle v. – обманывать, мошенничать

grafter n. – аферист, мошенник

testimony n. – заявление

penetrate v. – проникать

curiosity n. – любопытство

misdeed n. – преступление

ins-and-outs – все ходы и выходы

notorious adj.–пользующийся дурной славой

1. You are going to read the biographical part of the book “The Art of Deception” by the famous hacker and social engineer Kevin Mitnick. Work in groups of three: A, B, C. Read your text with the **Introduction** and **Final Thoughts** and find the best title for each part. Then make brief notes of your part.

1 Becoming a social engineer

2 Starting out

3 From phone phreak to hacker

INTODUCTION

Some hackers destroy people's files or entire hard drives; they're called crackers or vandals. Some novice hackers don't bother learning the technology, but simply download hacker tools to break into computer systems; they're called script kiddies. More experienced hackers with programming skills develop hackerprograms and post them to the Web and to bulletin board systems. And then thereare individuals who have no interest in the technology, but use the computer merely as a tool to aid them in stealing money, goods, or services.

Despite the media-created myth of Kevin Mitnick, I am not a malicious hacker.

But I'm getting ahead of myself.

Text A

My path was probably set early in life. I was a happy-go-lucky kid, but bored. After my father split when I was three, my mother worked as a waitress to support us. To see me then - an only child being raised by a mother who put in long, harried days on a sometimes-erratic schedule - would have been to see a youngster on his own almost all his waking hours. I was my own babysitter.

Growing up in a San Fernando Valley community gave me the whole of Los Angeles to explore, and by the age of twelve I had discovered a way to travel free throughout the whole greater L.A. area. I realized one day while riding the bus that the security of the bus transfer I had purchased relied on the unusual pattern of the paper-punch, that the drivers used to mark day; time, and route on the transfer slips. A friendly driver, answering my carefully planted question, told me where to buy that special type of punch.

The transfers are meant to let you change buses and continue a journey to your destination, but I worked out how to use them to travel anywhere I wanted to go for free. Obtaining blank transfers was a walk in the park.

The trash bins at the bus terminals were always filled with only-partly used books of transfers that the drivers tossed away at the end of the shifts. With a pad of blanks and the punch, I could mark my own transfers and travel anywhere that L.A. buses went. Before long, I had all but memorized the bus schedules of the entire system. (This was an early example of my surprising memory for certain types of information; I can still, today, remember phone numbers, passwords, and other seemingly trivial details as far back as my childhood.)

Another personal interest that surfaced at an early age was my fascination with performing magic. Once I learned how a new trick worked, would practice, practice, and practice some more until I mastered it. To an extent, it was through magic that I discovered the enjoyment in gaining secret knowledge.

Text B

My first encounter with what I would eventually learn to call social engineering came about during my high school years when I met another student who was caught up in a hobby called phone phreaking. Phone phreaking is a type of hacking that allows you to explore the telephone network by exploiting the phone systems and phone company employees. He showed me neat tricks he could do with a telephone, like obtaining any information the phone company had on any customer, and using a secret test number to make long-distance calls for free. (Actually it was free only to us. I found out much later that it wasn't a secret test number at all. The calls were, in fact, being billed to some poor company's MCI account.)

That was my introduction to social engineering-my kindergarten, so to speak. My friend and another phone phreaker I met shortly thereafter let me listen in as they each made pretext calls to the phone company. I heard the things they said that made them sound believable; I learned about different phone company offices, lingo, and procedures. But that "training" didn't last long; it didn't have to. Soon I was doing it all on my own, learning as I went, doing it even better than my first teachers.

The course my life would follow for the next fifteen years had been set. In high school, one of my all-time favorite pranks was gaining unauthorized access to the telephone switch and changing the class of service of a fellow phone phreak. When he'd attempt to make a call from home, he'd get a message telling him to deposit a dime because the telephone company switch had received input that indicated he was calling from a pay phone.

I became absorbed in everything about telephones, not only the electronics, switches, and computers, but also the corporate organization, the procedures, and the terminology. After a while, I probably knew more about the phone system than any single employee. And I had developed my social engineering skills to the point that, at seventeen years old, I was able to talk most telco employees into almost anything, whether I was speaking with them in person or by telephone.

My much-publicized hacking career actually started when I was in high school. While I cannot describe the detail here, suffice it to say that one of the driving forces in my early hacks was to be accepted by the guys in the hacker group.

Back then we used the term hacker to mean a person who spent a great deal of time tinkering with hardware and software, either to develop more efficient programs or to bypass unnecessary steps and get the job done more quickly. The term has now become a pejorative, carrying the meaning of "malicious criminal." In these pages I use the term the way I have always used it - in its earlier, more benign sense.

After high school I studied computers at the Computer Learning Center in Los Angeles. Within a few months, the school's computer manager realized I had found vulnerability in the operating system and gained full administrative privileges on their IBM minicomputer. The best computer experts on their teaching staff couldn't figure out how I had done this. In what may have been one of the earliest examples of "hire the hacker," I was given an offer I couldn't refuse: Do an honors project to enhance the school's computer security, or face

suspension for hacking the system. Of course, I chose to do the honors project, and ended up graduating cum laude with honors.

Text C

Some people get out of bed each morning dreading their daily work routine at the proverbial salt mines. I've been lucky enough to enjoy my work in particular you can't imagine the challenge, reward, and pleasure I had the time I spent as a private investigator. I was honing my talents in the performance art called social engineering (getting people to do things they wouldn't ordinarily do for a stranger) and being paid for it.

For me it wasn't difficult becoming proficient in social engineering. My father's side of the family had been in the sales field for generations, so the art of influence and persuasion might have been an inherited trait. When you combine that trait with an inclination for deceiving people, you have the profile of a typical social engineer.

You might say there are two specialties within the job classification of con artist. Somebody who swindles and cheats people out of their money belongs to one sub-specialty, the grifter. Somebody who uses deception, influence, and persuasion against businesses, usually targeting their information, belongs to the other sub-specialty, the social engineer. From the time of my bus-transfer trick, when I was too young to know there was anything wrong with what I was doing,

I had begun to recognize a talent for finding out the secrets I wasn't supposed to have. I built on that talent by using deception, knowing the lingo, and developing a well-honed skill of manipulation.

One way I worked on developing the skills of my craft, if I may call it a craft, was to pick out some piece of information I didn't really care about and see if I could talk somebody on the other end of the phone into providing it, just to improve my skills. In the same way I used to practice my magic tricks, I practiced pretexting. Through these rehearsals, I soon found that I could acquire virtually any information I targeted.

As I described in Congressional testimony before Senators Lieberman and Thompson years later:

I have gained unauthorized access to computer systems at some of the largest corporations on the planet, and have successfully penetrated some of the most resilient computer systems ever developed. I have used both technical and nontechnical means to obtain the source code to various operating systems and telecommunications devices to study their vulnerabilities and their inner workings.

All of this activity was really to satisfy my own curiosity; to see what I could do; and find out secret information about operating systems, cell phones, and anything else that stirred my curiosity.

FINAL THOUGHTS

I've acknowledged since my arrest that the actions I took were illegal, and that I committed invasions of privacy.

My misdeeds were motivated by curiosity. I wanted to know as much as I could about how phone networks worked and the ins-and-outs of computer security. I went from being a kid who loved to perform magic tricks to becoming the world's most notorious hacker, feared by corporations and the government. As I reflect back on my life for the last 30 years, I admit I made some extremely poor decisions, driven by my curiosity, the desire to learn about technology, and the need for a good intellectual challenge.

I'm a changed person now. I'm turning my talents and the extensive knowledge I've gathered about information security and social engineering tactics to helping government, businesses, and individuals prevent, detect, and respond to information-security threats.

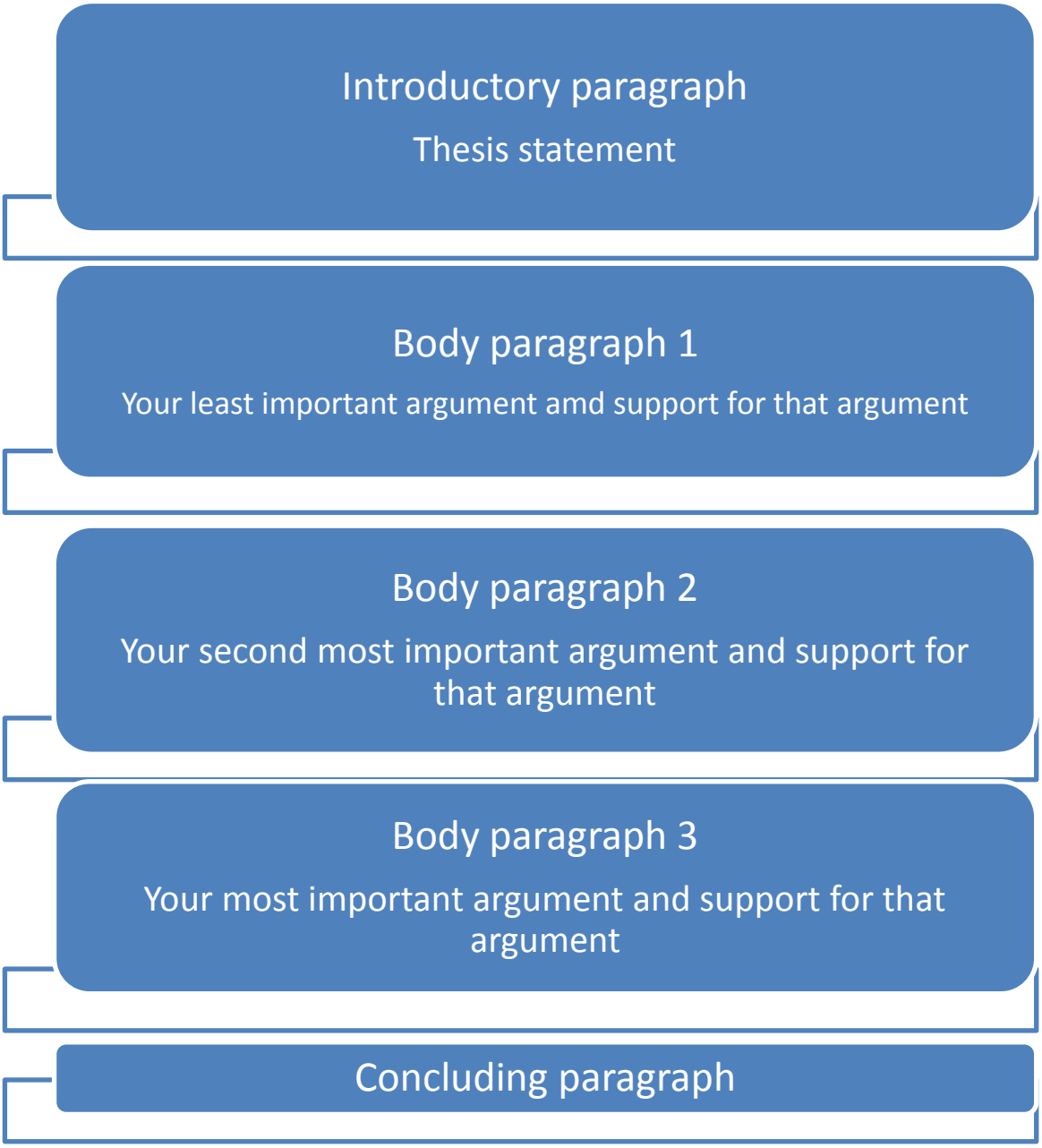
2. Now share information orally about your text with others in your group.

3. Look at the highlighted words and make up your own story om any topic using these words, the more – the better.

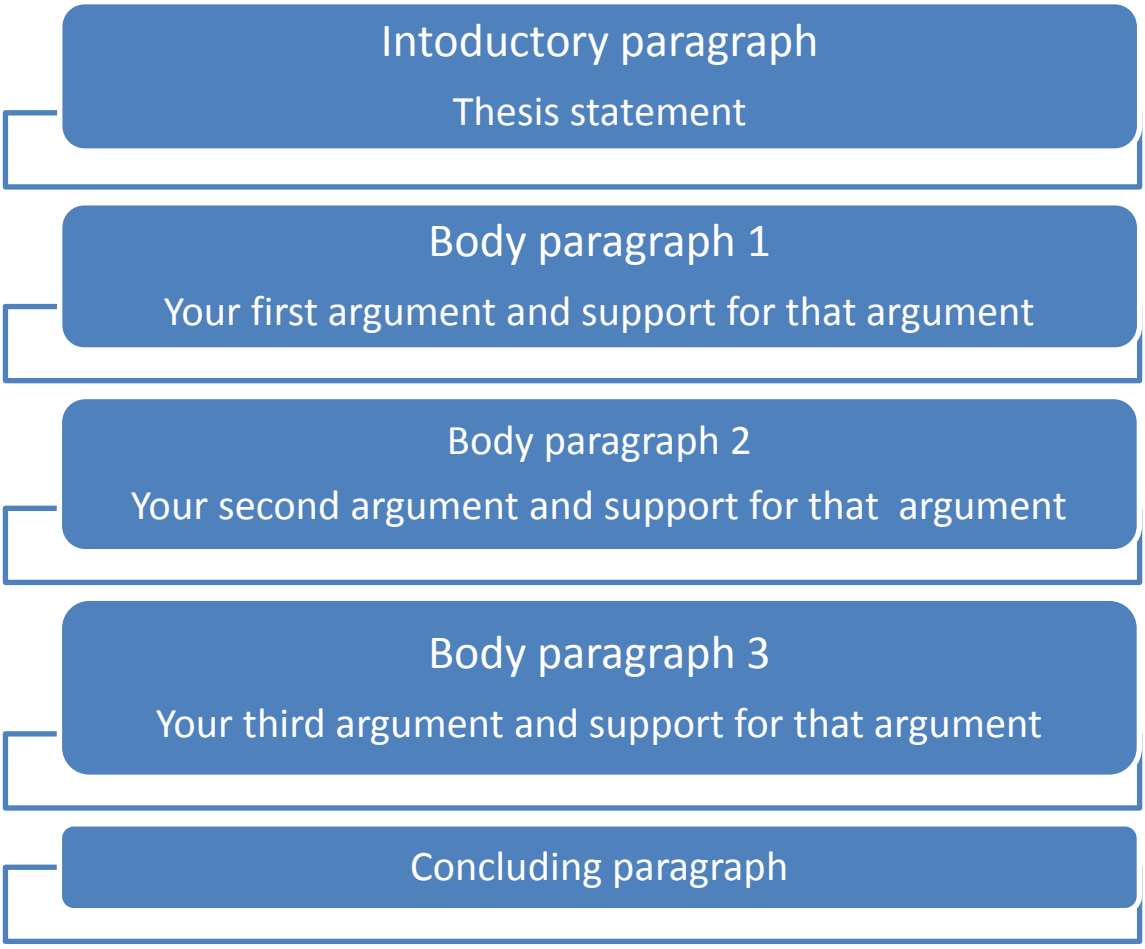
Writing

Graphic Organizers

Ascending Order



Equal Order



1. Ordering Arguments

   Below you will find a thesis statement and three arguments to support it. With a groupmate, discuss which of these arguments are more or less important. Put number 1 in front of the argument you think is most important, 2 in front of the second most important, and 3 in front of the least important argument. Then explain to the class why you ordered the arguments in this way.

Thesis statement: Electronic communication is hurting students' writing skills.

Arguments:

_____Because they depend on the spell checker, students aren't learning how to spell.

_____Students use the same casual style in their school papers as their e-mails.

_____Students use abbreviations and emoticons even in their academic essays.

2. Practicing Argumentation

   Below are two thesis statements. With one or two groupmates, discuss arguments that you can give to support each thesis statement. Then order them.

   1. Electronic communication is very useful for senior citizens.

   a. _____

   b. _____

   c. _____

   2. Electronic communication is good for the environment.

   a. _____

   b. _____

   c. _____

Model Essay 1

Everyone is Talking, and No One is Listening

Since the middle of the 1990s, the ability to communicate electronically has expanded dramatically. Electronic communication is changing how people relate to one another. However, one thing remains constant: There new forms of communication are not face to face. They are distant, and they keep people at a distance. In my opinion, due to electronic communication, relationships today are changing for the worse; they have become fragmented, superficial, and anonymous.

Communication these days is becoming a process of exchanging messages of two or three words. There is no longer time for serious and deep reflection.

For example, in most countries, sending a text message via a cell phone is much cheaper than talking on that phone, so people send each other silly messages like "RU ready?" or "4 sure". The language of Shakespeare and Milton has become reduced to abbreviations. With Instant Messenger (IM), people send each other emoticons such as a smiley face instead of sentences. There is no give-and-take. These fragmented messages are not true communication.

The current ability to relate to one another electronically is largely textual; that is, people read messages from each other. Blogs, or Web logs, have become the way to communicate. However, anyone, anywhere can create a blog, and they can write anything they want. There are millions of blogs being produced. It seems that everyone wants to shout, "Hey, here I am! This is me!", but no one really listens.no one responds. Another reason why relationships are becoming more superficial is the spread of e-mail. It's impossible to have a serious discussion with people through e-mail. Because they are overwhelmed by spam in addition to real messages, people just skim what they see and either make a rapid, thoughtless response or ignore it completely. No one reads e-mail messages carefully because there are just too many of them.

Finally, while one great advantage of the World Wide Web is that it is anonymous, this is also its major disadvantage. Anyone can pretend to be anyone. For example, a sixteen-year-old high school student could say that he isa twenty three-year-old college graduate, and the person reading his blog or profile would never know. This type of anonymity can also put Internet users at risk. There are many news stories about a criminal convincing a teenage to meet him at a coffee shop or a mall. The teenager agrees to meet her Internet friend because she thinks she is meeting another teenager. The Web knows no one; a person can invent an identity. It's clear that there can be np real communication when it's so easy for someone to remain anonymous.

In short, electronic communication has multiple advantages, but it also has disadvantages. This new form of communication makes people lonelier because they don't make real and meaningful connections. The communication is

fragmented and superficial, and it is not always honest because of the ability to be anonymous. Fewer silly messages and more face-to-face communication would make us better people, I think.

3. Analyzing Model Essay 1

   With a groupmate, discuss the answers to these questions.

   1. Which organizational pattern does this essay follow? (Check one.)
      a. ascending order
      b. equal order
   2. What is the thesis statement?
   3. The first body paragraph supports the opinion that electronic communication has made our relationships more fragmented. Give an example of each of the communication methods the author mentions:
      a. abbreviations
      b. emoticons
   4. How do the author's examples of blogs and the increase of e-mail support the second opinion that electronic communication is superficial? Give two examples.
      a. _____
      b. _____
   5. Give two examples in the essay to support the author's third argument that electronic communication makes people anonymous.
   6. Do you think this essay is convincing? Why or why not?

Model Essay 2

Dating in Cyberspace

The number of single people in the United States has been increasing for several years. Many of them like being single and do not want to find a marriage partner. Some, however, want to find someone, but they're too busy to spend the

time. They don't want to invest time in a relationship, find out that they aren't compatible, and have to start all over again. There is a solution to this problem: cyberdating. Anyone who is seriously looking for a partner should try cyberdating.

For one thing, cyberdating is extremely convenient. There are many reputable websites that make it easy to post your profile for others to see. Once you have posted your profile, you read about the thousands of others who have done the same. You can take us much or as little time as you like looking through the database. Also, these sites are available 24 hours a day, so you can search when you have the time.

Furthermore, cyberdating can keep you from being hurt. Too often on a first date, you see boredom or disappointment in your date's eyes. All you can do in this situation is to persevere and hope the date ends early. With cyberdating, however, the people you decide to meet have already seen a photo of you, and they already know a lot about you. There is no surprise, so there is no disappointment. In fact, it's just the opposite. You and your date are excited to meet each other, and you look at each other with hope.

Finally, the anxiety of dating is greatly lessened with cyberdating. Traditionally, men take the lead in dating. They are the ones who have to ask a woman out on a date. They have to risk rejection. It's no better for women, however. Many women still wait for a man to ask them out first. Then, if they don't want to go out with him, they have to let the man down gently. While it's true that sometimes with cyberdating men still get rejected and women still reject, you experience this in the privacy of your own home. Moreover, you never have to see the person again because you have never met! It's the perfect solution.

In short, if you are looking for someone to date and even marry, you should go online and post your profile on a dating website. It's convenient, safe, and worry-free.

4. Below are three other topics for a persuasive essay about electronic communication.

    1.Online education is as good as/better than/worse than education in a classroom.

    2.Making friends on the Web is dangerous/not realistic/better than trying to meet people face to face.

    3.Online newspapers are better/worse than paper ones.

Role-play

Participants:

Interviewer

Hacker

Work in pairs. Together make up your own questions on these prompts. Then play the parts of the interviewer and the hacker.

1. first interested in hacking
2. reason for being arrested
3. present job
4. ways to avoid hackers
5. views on Hollywood hackers
6. safe ways of paying for Internet shopping

Assignments for Self-Evaluation: Examination Paper Sample

<u>Vocabulary Test</u>

Complete the passage with the best option from the list below.

As much as everyone hates to think about this, it is a reality that we all must face: 1)_____are not going to stop, and everyone is a target. It may even be safe to say that any person who has even briefly gone on the Internet has been exposed to some cyber threat, whether it is 2)_____or 3)_____. 4)_____ attack organizations just as much if not more than individuals. Large-scale attacks like 5)_____ are especially appealing to 6)_____because they can steal way more information in less time by infiltrating centralized locations like corporate databases than they would 7)_____individuals one by one. News of such mass attacks not only make headlines but strike chords with many, as household names Target and Chase Bank 8)_____ by cyber attacks. Retail giant Target suffered a breach in 2013 that 9)_____the credit and debit card information of 70 million customers. The Chase Bank breach in 2014 10)_____over 83 million accounts that included 76 million households and 7 million small businesses.

1.	a)	cyberattacks	b)	crimes	c)	bloody murders
2.	a)	a birthday present	b)	a parcel	c)	a phishing email
3.	a)	malware download	b)	software	c)	hardware
4.	a)	criminals	b)	hackers	c)	robots
5.	a)	data breaches	b)	personal losses	c)	bloody murders
6.	a)	pretty women	b)	cyber thieves	c)	children
7.	a)	send	b)	get	c)	target
8.	a)	were burgled	b)	were destroyed	c)	were victimized
9.	a)	compromised	b)	closed	c)	attacked
10.	a)	hacked	b)	killed	c)	impacted

Grammar

Choose the correct option.

1. They wanted to build a machine ……. people could use to talk over long distances.
   a. what b. which c. who

2. Currently intensive work and research …….. on new robots in many countries.
   a. are being carried out b. are carried out c. carrying out

3. Such data is used …….. decisions that can impact our lives for better or worse.
   a. making b. to make c. make

4. Instead of a worm simply interfering one system it will enable …… compromise of the system.
   a. further b. farer c. more far

5. If we had got a good understanding of the basics of information security, we ……..with all occurred problems.
   a. will cope b. would cope c. would have coped

6. Many security products now incorporate …….. such as antivirus.
   a. defensive measures multiple b. multiple defensive measures
   b. measures defensive multiple

7. Good specialists ……. to know their specialization quite well in order to be in demand.
   a. ought b. should c. must

8. ID-related data theft occurs when customer records are stolen or …….. copied.

a. illegally b. unlegally c. disligally

9. …… people understand this application.
   a. little b. small c. few

10. I …… my work by 5 o'clock.
    a. completed b. have completed c. had completed

Reading Comprehension

Read the text and answer the questions below

The CIA Triad

The CIA triad is a very important trio in information security. The "CIA" stands for Confidentiality, Integrity, and Availability. These are the three elements that everyone in the industry is trying to protect. Let's touch on each one of these briefly.

Confidentiality: Protecting confidentiality deals with keeping things secret. This could be anything from a company's intellectual property to a home user's photo collection. Anything that attacks one's ability to keep private that which they want to is an attack against confidentiality.

Integrity: Integrity deals with making sure things are not changed from their true form. Attacks against integrity are those that try and modify something that's likely going to be depended on later. Examples include changing prices in an ecommerce database, or changing someone's pay rate on a spreadsheet.

Availability: Availability is a highly critical piece of the CIA puzzle. As one may expect, attacks against availability are those that make it so that the victim cannot use the resource in question. The most famous example of this sort of attack is the denial of service attack. The idea here is that nothing is being stolen, and nothing is being modified. What the attacker is doing is keeping you

from using whatever it is that's being attacked. That could be a particular server or even a whole network in the case of bandwidth-based DoS attacks.

It's a good practice to think of information security attacks and defenses in terms of the CIA triad. Consider some common techniques used by attackers — sniffing traffic, reformatting hard drives, and modifying system files.

Sniffing traffic is an attack on confidentiality because it's based on seeing that which is not supposed to be seen. An attacker who reformats a victim's hard drive has attacked the availability of their system. Finally, someone writing modified system files has compromised the integrity of that system. Thinking in these terms can go a long way toward helping you understand various offensive and defensive techniques.

1. What does the "CIA" stand for?
2. What elements in Information Security industry must be protected?
3. What does protecting confidentiality deal with?
4. What does integrity deal with?
5. What is availability in terms of Information Security?
6. What is the most famous example of attack against availability?
7. What is the effect of DoS attack?
8. What are common techniques used by attackers? Describe one of them.

Speaking

Speak on one of the following topics. You should speak for 3-5 minutes. You have 10 minutes to prepare your speech.

1. Physical information security
2. Cryptography
3. My future profession (Information Security Department)

ГЛОССАРИЙ. GLOSSARY

abuse *n*	нарушать режим эксплуатации
accessible *adj*	доступный
alter *v*	изменять
back up *n*	резервное копирование
brute-forcing *n*	грубый метод
bug *n*	ошибка
capability *n*	техническая возможность
cash flow	движение денежной наличности
combat *v*	оказывать противодействие
consent *n*	согласие, разрешение
corruption *v*	повреждение
data breach	утечка данных
eavesdropping *n*	несекционное извлечение информации
employ *v*	использовать
employee *n*	сотрудник
evidence *n*	доказательство, улика
execute *v*	выполняться
forceful *adj*	принудительный
fraudulent *adj*	мошеннический
inadvertently *ad*	непреднамеренно, без умысла
install *v*	устанавливать
instant message	мгновенное сообщение
intended users	предполагаемые пользователи
issue *n*	проблема
lack *n*	недостаток, нехватка
launch *n*	запускать
malicious *adj*	вредоносный
masquerade *v*	выдавать себя за кого-то, притворяться

metadata *n*	метаданные, данные о данных
on-demand	запрашиваемый
penetration *n*	проникновение
plain text	открытый текст, нешифрованный
productive *adj*	полезный
property *n*	собственность, имущество
realm *n*	область, сфера
replicate *v*	копировать
respectively *ad*	соответственно
reveal *v*	рассекретить
sensitive *adj*	важный, конфиденциальный
solid *adj*	глубокий
spyware *n*	шпионское программное обеспечение
target *n*	цель
utilize *v*	использовать
valuable *adj*	ценный
vulnerable *adj*	уязвимый
vulnerability *n*	уязвимость

ЗАКЛЮЧЕНИЕ

Учебное пособие направлено на применение практических навыков иноязычной коммуникативной компетенции у студентов 3 курса «Информационная безопасность». Тщательно отобранный аутентичный материал пособия и упражнения, направленные на развитие и углубление всех видов речевой деятельности в сфере профессиональной коммуникации, способствуют успешному обучению студентов. Пособие предназначено для основной и дополнительной работы студентов.

Данное пособие составлено авторами таким образом, чтобы была четкая и логичная организация представленного материала: первые два модуля состоят из первого опорного текста (1A, 2A), разделов Language Focus (работа с лексикой) ,Listening (основаны на лекциях Tedtalks), Writing, Case Study, Grammar, Role-Play, текстов ознакомительного характера (1B, 1C, 2B, 2C) и раздела Assignments for Self-Evaluation: Examination Paper Sample, в котором содержатся задания в формате экзамена.

Учебное пособие нацелено на закрепление и совершенствование всех видов речевой деятельности, которые представляют собой чтение, аудирование, говорение и письмо. То есть данное пособие представляет собой переход от общенаучной сферы коммуникации (1 и 2 курсы обучения) к узкоспециальной (3 курс).

В результате изучения дисциплины «Иностранный (английский) язык» в области информационной безопасности у студентов формируются профессиональные компетенции в профессиональной деятельности благодаря расширению их возможностей использовать англоязычные аутентичные источники и приобретенные языковые навыки в профессиональном и деловом общении на английском языке.

Более того, пособие соответствует всем современным стандартам согласно последним тенденциям методики обучения иностранному языку:

развитие всех аспектов речевой деятельности, коммуникативные и интерактивные задания (кейс-задачи, ролевые игры). Аудирование построено на основе научно-популярных лекций TedTalks, которые на сегодняшний день являются образцами научного ораторского дискурса. В целом, авторы пособия постарались сделать его современным, интерактивным и мотивирующим, чтобы помимо основных заявленных компетенций развивать также у студентов творческие и креативные навыки.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Андреев А. Л. Инновационный путь развития России в контексте глобального пространства образования. //Вестник Российской Академии наук, 2010. — Т. 80. — № 2. — С. 99–106.
2. Байденко В. И. Компетенции: к освоению компетентностного подхода // Труды методологического семинара«Россия в Болонском процессе: проблемы, задачи, перспективы». / В.И Байденко. — М.: Исследовательскийцентр проблем качества подготовки специалистов, 2004. — с. 25–30.
3. Долгоруков А. М. Casestudy как способ понимания // Практическое руководство для тьютера системы Открытого образования на основе дистанционных технологий. М.: Центр интенсивных технологий образования, 2002. С. 21-44.
4. Покушалова Л. В. Метод case-study как современная технология профессионально-ориентированного обучения студентов // Молодой ученый, 2011. № 5. Т. 2. С. 155-157.
5. Beaver K. Hacking for Dummies. 4th edition, 2013. 408 p.
6. Doodly J., Evans V. Grammarway 4. Express Publishing, 2006, 224 p.
7. Murphy R. English Grammar in Use: A Self-study Reference and Practice Book for Intermediate learners of English. Cambridge University Press, 2012. 380 p.
8. Obee B., Evans V. Upstream. Upper –Intermediate. Student’s book. Express Publishing, 2003, 264 p.
9. Obee B., Evans V. Upstream. Upper –Intermediate. Workbook. Express Publishing, 2003, 264 p.

СПИСОКИНТЕРНЕТ-ИСТОЧНИКОВ

1. Демкин В.П. Инновационные технологии в образовании. Электронныйресурс. Режим доступа: http://www.center-

yf.ru/data/stat/Innovacionnye-tehnologiiv-obrazovanii.php (дата обращения 06.04.2018).

2. Инновационные технологии в образовании. Электронный ресурс.Режим доступа: http://www.center-yf.ru/data/stat/Innovacionnye-tehnologii-vobrazovanii.php (дата обращения 06.04.2018).
3. Современные образовательные технологии. Электронный ресурс.Режим доступа: http://karpinsk-edu.ru/resources/mediateka/1720-sovrobraztech(дата обращения 03.11.2013).
4. CVE Details. The Ultimate Security Vulnerability Datasource. URL: https://www.cvedetails.com/ (accessed on 10.05.2018).
5. Hacker News – Most Popular Cyber Security, Hacking News Site. URL:https://thehackernews.com/search?updated-max=2018-01-05T01:24:00-11:00&max-results=5&start=5&by-date=false&m=1 (accessed on 10.05. 2018).
6. TedTalks. All your devices can be hacked URL: https://www.ted.com/talks/avi_rubin_all_your_devices_can_be_hacked/transcript?referrer=playlist-who_are_the_hackers#t-997135/(accessed on 14.06.2018).
7. TedTalks. Hackers: the Internet's Immune System. URL:https://www.ted.com/talks/keren_elazari_hackers_the_internet_s_immune_system/transcript (accessed on 14.06.2018).
8. ZDnet.URL:https://www.zdnet.com/article/what-is-malware-everything-you-need-to-know-about-viruses-trojans-and-malicious-software/(accessed on 14.06.2018).

Электронные словари

1. Multitran. URL: http://www.multitran.com/
2. ABBY Lingvo Live. URL: https://www.lingvolive.com/ru-ru
3. Cambridge Dictionary https://dictionary.cambridge.org/dictionary/english/
4. Longman Dictionary of Contemporary English

https://www.ldoceonline.com/

5. Collins English Dictionary https://www.collinsdictionary.com/dictionary/english/english

ПРИЛОЖЕНИЯ.

APPENDIX 1.

TESTS

VOCABULARY

Vocabulary Test 1

Matching questions

1. ☐
   запрашиваемый
2. ☐
   уязвимость
3. ☐
   вредоносный
4. ☐
   уязвимый
5. ☐
   доступный

A. vulnerability

B. on-demand

C. accessible

D. malicious

E. vulnerable

Multiple choice questions

1. мошеннический

1. forceful
2. fraudulent

2. penetration

1. on-demand

3. penetration

1. шпионское ПО
2. мошеннический
3. вредоносный
4. проникновение

4. cashflow

1. резервное копирование
2. движение денежной наличности
3. вредоносный
4. техническая возможность

5. forceful

1. принудительный
2. вредоносный
3. мошеннический
4. запрашиваемый

6. запускать

1. employ
2. target
3. launch
4. utilize

True/False questions

1. собственность, имущество → property
   True False
2. цель → launch
   True False
3. техническая возможность → capability
   True False
4. несекционное извлечение информации → eavesdropping
   True False
5. issue → использовать
   True False

Vocabulary Test 2

Matching questions

1. ☐
malicious

2. ☐
capability

3. ☐
penetration

4. ☐
brute-forcing

5. ☐
utilize

6. ☐

vulnerable

7. ☐

vulnerability

A. использовать

B. вредоносный

C. уязвимость

D. проникновение

E. грубый метод

F. уязвимый

G. техническая возможность

Multiple choice questions

Multiple choice questions

1. employee

1. ○ шпионское ПО
2. ○ доступный
3. ○ сотрудник
4. ○ использовать

2. проблема

1. ○ issue
2. ○ spyware
3. ○ utilize
4. ○ abuse

3. cash flow

1. ○ движение денежной наличности
2. ○ резервное копирование

3. вредоносный
4. техническая возможность

4. employ

1. использовать
2. шпионское ПО
3. запускать
4. сотрудник

5. цель

1. issue
2. launch
3. employ
4. target

6. abuse

1. движение денежной наличности
2. нарушать режим эксплуатации
3. проблема
4. резервное копирование

7. spyware

1. проникновение
2. использовать
3. запрашиваемый
4. шпионское ПО

True/False questions

1. мошеннический → fraudulent

   True False

2. собственность, имущество → property

   True False

3. on-demand → мошеннический

   True False

4. принудительный → malicious

   True False

5. eavesdropping → несекционное извлечение информации

   True False

6. запускать → employ

   True False

Vocabulary Test 3

Matching questions

1.

alter

2.

valuable

3.

target

4.

solid

5.

reveal

6.

execute

7.

replicate

A. глубокий

B. копировать

C. выполняться

D. изменять

E. рассекретить

F. ценный

G. цель

Multiple choice questions

1. malicious

1. вредоносный
2. доступный
3. копировать
4. повреждение

2. метаданные, данные о данных

1. property
2. metadata
3. sensitive
4. evidence

3. доказательство, улика

1. consent
2. evidence
3. metadata
4. property

4. inadvertently

1. непреднамеренно, без умысла
2. предполагаемые пользователи
3. открытый текст, нешифрованный
4. соответственно

5. spyware

1. ○ оказывать противодействие
2. ○ устанавливать
3. ○ согласие, разрешение
4. ○ шпионская программа

6. мгновенное сообщение

1. ○ intendedusers
2. ○ inadvertently
3. ○ respectively
4. ○ instant message

7. intended users

1. ○ предполагаемые пользователи
2. ○ мгновенное сообщение
3. ○ непреднамеренно, без умысла
4. ○ открытый текст, нешифрованный

True/False questions

1. выдавать себя за кого-то, притворяться → plaintext
   ○ True ○ False
2. устанавливать → install
   ○ True ○ False
3. consent → доказательство, улика
   ○ True ○ False
4. property → собственность, имущество
   ○ True ○ False
5. соответственно → productive

True False False

Vocabulary Test 4

Matching questions

1.
мошеннический
2.
полезный
3.
изменять
4.
вредоносный
5.
доступный
6.
цель
7.
ценный

A. valuable
B. productive
C. accessible
D. target
E. alter
F. fraudulent
G. malicious

Multiple choice questions

1. **solid**

1. полезный
2. изменять
3. вредоносный
4. глубокий

2. **открытый текст, нешифрованный**

1. inadvertently
2. property
3. fraudulent
4. plaintext

3. **install**

1. область, сфера
2. копировать
3. рассекретить
4. устанавливать

4. **execute**

1. выполняться
2. полезный
3. копировать
4. вредоносный

5. **reveal**

1. копировать
2. рассекретить
3. область, сфера
4. устанавливать

6. **оказывать противодействие**

1. spyware
2. property
3. consent
4. combat

7. **inadvertently**

1. предполагаемые пользователи
2. соответственно
3. открытый текст, нешифрованный
4. непреднамеренно, без умысла

True/Falsequestions

1. realm → область, сфера
   True False
2. предполагаемые пользователи → inadvertently
   True False
3. spyware → согласие, разрешение
   True False
4. ошибка → bug
   True False
5. metadata → метаданные, данные о данных
   True False

Vocabulary Test

Complete the passage with the best option from the list below.

Cryptography involves creating written or generated codes that allow information to be kept1_____. Cryptography converts data into a format that is unreadable for an 2_____ user, allowing it to be transmitted without unauthorized entities decoding it back into a 3_____format, thus compromising the data.

Information 4_____ uses cryptography on several levels. The information cannot be read without a key to decrypt it. The information maintains its integrity during transit and while being stored. 5_____also aids in nonrepudiation. This means that the sender and the delivery of a message can be verified.

Cryptography is also known as cryptology.

Cryptography also allows senders and receivers to authenticate each other through the use of key pairs. There are various types of algorithms for encryption, some common algorithms include:

Secret Key Cryptography (SKC): Here only one 6_____is used for both encryption and decryption. This type of encryption is also referred to as7_____.

Public Key Cryptography (PKC): Here two keys are used. This type of encryption is also called asymmetric encryption. One key is the public key that anyone can access. The other key is the 8_____key, and only the owner can access it. The sender encrypts the information using the receiver's public key. The 9_____decrypts the message using his/her private key. For nonrepudiation, the sender encrypts plain text using a private key, while the receiver uses the sender's public key to decrypt it. Thus, the receiver knows who sent it.

Hash Functions: These are different from SKC and PKC. They use no key and are also called one-way encryption. Hash functions are mainly used to ensure that a file has remained10_____.

1.	a)	closed	b)	secret	c)	evident
2.	a)	unauthorized	b)	authorized	c)	unknown
3.	a)	readable	b)	clear	c)	interesting
4.	a)	protection	b)	security	c)	awareness
5.	a)	Information security	b)	Analysis	c)	Cryptography
6.	a)	key	b)	person	c)	attempt
7.	a)	symmetric encryption	b)	asymmetric encryption	c)	hide-and-sick encryption
8.	a)	private	b)	my	c)	useful
9.	a)	sender	b)	person	c)	receiver
10.	a)	hacked	b)	unchanged	c)	impacted

READING COMPREHENSION

Read the text and answer the questions below

Difference between a vulnerability assessment and a penetration testing

What's the difference between a vulnerability assessment and a penetration test? The answer to that question depends on who you choose to ask. For some people they are effectively one and the same thing; for others there are clear distinctions. So what's the true position? Are vulnerability assessments and penetration test effectively two sides of the same coin, or are there clear differences between the two? The short answer is that whilst a penetration test may be a form of vulnerability assessment, a vulnerability assessment is definitely not a penetration test.

Vulnerability Assessments

A vulnerability assessment is the process of running automated tools against defined IP addresses or IP ranges to identify known vulnerabilities in the environment. Vulnerabilities typically include unpatched or misconfigured systems. The tools used to run vulnerability scans may be commercially available versions, or free open-source tools.

The commercial versions typically include a subscription to maintain up-to-date vulnerability signatures similar to software subscriptions. These tools provide a straight-forward method of performing vulnerability scanning. Organizations may also choose to use open-source versions of vulnerability scanning tools. The principle advantage of open-source tools is that they allow you to use the same tools of the trade as hackers: after all hackers are unlikely to pay an expensive subscription when they can download tools free. The advantage of using a commercially licensed vulnerability scanner is that there will be a low risk that malicious code is included in the tool.

The purpose of a vulnerability scan is to identify known vulnerabilities so they can be fixed, typically through the application of vendor-supplied patches. Vulnerability scans are critical to an organizations' vulnerability management program. The scans are typically run at least quarterly, though many experts would recommend monthly scans.

Penetration Tests

A penetration test takes the vulnerability assessment to a different level. One of the initial phases performed by a penetration tester is to perform a vulnerability scan to learn the IP addresses, device type, operating systems and vulnerabilities present on the systems, however unlike the vulnerability scan, the penetration tester does not stop there. The next phase of a penetration test is exploitation which takes advantage of the vulnerabilities identified in the system to escalate privileges to gain control of the network or to steal sensitive data from the system. The exploitation phase also uses automated tools which the penetration tester can configure to execute automated exploits against the systems. Experienced penetration testers will also perform manual exploits of the systems vulnerabilities.

Penetration tests are categorized as white box or black box tests. White box tests are performed with full knowledge of the target company's IT Department. Information is shared with the tester such as network diagrams, IP addresses and system configurations. The white box approach tests the security of the

underlying technology. The black box test closely represents a hacker attempting to gain unauthorized access to a system. The IT Department is unaware a test is being performed and the tester is not provided detailed information about the target environment. The black box method of penetration testing evaluates both the underlying technology and the people and processes in place to identify and block a real world attacks.

Both the vulnerability assessment and penetration test should be performed against the internal and external servers and network devices. Testing the external interfaces simulates a hacker attempting to gain access from the Internet through publicly available interfaces. The internal test simulates a rogue employee or unauthorized user who has access to the internal network attempting to escalate their privileges to gain access to internal systems or data.

Although vulnerability assessments and penetration testing have different goals, both should be performed to improve the overall security of the information system by a skilled information security professional. The vulnerability assessment should be performed regularly to identify and fix known vulnerabilities on an on-going basis. The penetration test should be performed by a skilled and experienced penetration tester at least once a year and definitely after significant changes in the information systems environment to identify exploitable vulnerabilities in the environment that may give a hacker unauthorized access to the system.

1. What may a penetration test be?
2. What is a vulnerability assessment?
3. What do vulnerabilities typically include?
4. What tools are used to run vulnerability scans?
5. What is the principle advantage of open-source tools?
6. What is the advantage of using a commercially licensed vulnerability scanner?
7. What is the purpose of a vulnerability scan?
8. What are two initial phases performed by a penetration tester?

9. How can be penetration tests categorized?
10. What are white box tests and black box tests?
11. Why should both the vulnerability assessment and penetration test be performed against the internal and external servers and network devices?
12. How often should the vulnerability assessment and penetration test be performed?

GRAMMAR

Choose the correct option.

1. The scientist about …… we heard so much came to our country.
   a. which b. whom c. what

2. During the course of study students ……. practical work in well-equipped laboratories.
   a. are carrying out b. carry out c. will carry out

3. In most cases it is better ….. a backup of everything on the compromised system's hard drive.
   a. to make b. making c. make

4. The impact of compound defenses seems …….. substantial than the effect of compound attacks.
   a. less b. little c. littler

5. Every page on your site ……accessible from every other one within four clicks.

should to be b. need be c. should be

6. If the information on the systems …… to an attacker, the consequences can be bad indeed.
   a. will become exposed b. becomes exposed c. become exposed

7. The information …….. in this book can be very useful.
   a. provided b. providing c. provides

8. It is evident to all that an old ……. power station is more dangerous and must be destroyed.
   a. efficient b. inefficient c. unefficient

9. A…… includes its employee records.
   a. confidential company's information b. company's information confidential
   b. company's confidential information.

10. We are sure that we ……our project by 7 pm tomorrow.
   a. will do b. are going to do c. will have done

APPENDIX 2.

TOPICS.

Cybercrime

Cybercrime can be defined as any criminal activity in which a computer (or networked device) is targeted and/or used. Some cybercrimes directly attack a computer or device in order to damage or disable it. Others make use of a computer to spread malware, illegal information, images or other materials. Cybercrimes often do both, for example targeting a computer in order to infect it with a virus which is then spread to other machines.

Categorizing cybercrimes can be difficult since there is considerable overlap. However, most cybercrimes can be broadly divided into four types: These are two of these types.

Finance-related Cybercrime

Unsurprisingly, many criminals turn to the internet in order to make money at the expense of others.

Online Phishing Scams

Cybercriminals like to target the low-lying fruit and if they can entice an unsuspecting victim into downloading a virus then they will. Phishing emails are a favorite tool of the scammer. These persuade the recipient into clicking a link by posing as a legitimate company or organization (a bank, tax company, popular e-commerce store, etc.) Such scams are often used to obtain bank details.

Cyberextortion

Another popular method of finance-related cybercrime is cyberextortion. This is where an individual or company are locked out of their files, usually by inadvertently downloading malware. The cybercriminal will then offer to restore

the files in return for a payment, usually in the form of a cryptocurrency such as Bitcoins.

Financial Fraud

More sophisticated financial fraud includes hacking retailers computer systems to obtain customers' bank details (e.g. the Target attack) and diverting or manipulating financial data. Some types of financial fraud can be extremely hard to detect.

Privacy-related Cybercrime

There are a number of different types of cybercrime designed to undermine privacy protection. Although most of these crimes are ultimately driven by a deeper motive (e.g. to make money or drive political change), their main focus is on getting around laws and technologies put in place to protect our right to privacy.

Identity Theft

Identity theft involves the personification of one person or group by another. Although some criminals will steal an ID in order to physically represent another person, for example by obtaining and using a passport, much identity theft is conducted purely online.

For example, an ineligible person or organisation wanting to access a bank loan may steal the identity of someone with a good credit rating.

Espionage

From illegal mass surveillance to hacking an individual computer or connected device, this group of cybercrimes is designed to secretly monitor our behavior. It includes everything from physical spying (e.g. using a webcam or CCTV camera to watch a targeted individual or group) to mass communications monitoring (recording and/or storing emails, text messages, Instant Messages, etc.)

Copyright Infringement

One of the most widespread forms of cybercrime is copyright infringement. This includes the sharing of works of art (music, photography, movies, books, etc.) on the internet without the permission of the copyright owner.

Spam

Sending spam is deemed a cybercrime in some areas. Spam can include emails, SMS messages, Instant Messages and other types of communication. Whether the content is pure junk or a well-designed newsletter is irrelevant; any message which is sent in bulk to recipients who haven't asked for it is by definition spam.

Means of Attack

There are four common means of attack in cybercrime.

The first many people fear is a technological exploitation using some kind of malware (virus, trojan, worm, etc.). Experts understand many different ways in which systems can be exploited and how it is important to follow robust security protocols such as using strong passwords and promptly installing software updates. This means of attack is focused on misusing computers and networks.

The second means of attack is the distributed denial-of-service (DDOS) attack which uses a network's own communications protocol against it by overwhelming its ability to respond to connection requests. This means of attack is focused on shutting down computers and networks.

The third means of attack involves a powerful combination of social engineering and malicious coding. Best known in the form of phishing, this method persuades an individual to perform a certain behavior (clicking a link on an email, visiting a website, etc.) which then opens up their device to infection using the first means of attack.

The fourth means of attack, used by those who want to conduct illegal activity such as harassment, trafficking, grooming or distributing illegal content consists

of subversion. These cybercriminals cover their tracks by using anonymous profiles, encrypted messaging services and other identity-hiding technologies.

As you can see, cybercrime encompasses a wide range of illicit activities from fraud and identity threat to hate crime and drug trafficking. It can be difficult to neatly divide cybercrime into types because there is considerable overlap. For example, a phishing attack may initially be used for identity theft. However, this fake identity may then be used for obtaining money or a passport to aid drug traffickers or terrorists. It is important to understand that cybercrime is not always about complicated hacking and does not only take place in the 'dark web'. The best form of defense against cyberattack is to remain informed and up-to- date about the latest threats.

Anti-virus software

Anti-virus software is a program or a set of programs that are designed to prevent, search for, detect, and remove software viruses, and other malicious software like worms, trojans, adware, and more.

These tools are critical for users to have installed and up-to-date because a computer without anti-virus software installed will be infected within minutes of connecting to the internet. The bombardment is constant, with anti-virus companies update their detection tools constantly to deal with the more than 60,000 *new* pieces of malware created daily.

There are several different companies that build and offer anti-virus software and what each offers can vary but all perform some basic functions:

- Scan specific files or directories for any malware or known malicious patterns
- Allow you to schedule scans to automatically run for you
- Allow you to initiate a scan of a specific file or of your computer, or of a CD or flash drive at any time.

- Remove any malicious code detected – sometimes you will be notified of an infection and asked if you want to clean the file, other programs will automatically do this behind the scenes.
- Show you the 'health' of your computer

Always be sure you have the best, up-to-date security software installed to protect your computers, laptops, tablets and smartphones.

Physical information security

STOP. THINK. CONNECT?

As weird as it might seem, there are physical aspects to securing information about you: **Before your data are stolen or corrupted,** there's a need to keep track of devices and media containing information about you and your life. **After someone acquires your data,** there's the possibility it could be used against you in the real world (online banking theft, physical robbery, extortion, and, in extreme cases, physical violence).

We encourage you to STOP before leaving your laptop or phone behind in a public area during trips to the restroom; before tossing your class schedule into the recycle bin unshredded; before posting information about your physical location, upcoming vacation (OK to post *afterwards!*), or financial habits.

Then THINK about the possible implications of this action; whether the links in that email or text message point to an official UVM website; whether you even have an account with that bank; whether Facebook is really likely to have forgotten how to use spell-check.

Finally, CONNECT with your surroundings, both virtual and physical: Is this a safe place to leave my laptop? Does this website seem sketchy?

A tiny pause can mean the difference between an enjoyable experience and a messy situation. It may seem like a lot to ask, but while we can't claim this will make you invulnerable, it won't be long before you don't even realize you're doing it.

Cryptography

Cryptography is closely related to the disciplines of cryptology and cryptanalysis. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as cryptographers.

Modern cryptography concerns itself with the following four objectives:

1) **Confidentiality** (the information cannot be understood by anyone for whom it was unintended)

2) **Integrity** (the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected)

3) **Non-repudiation** (the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information)

My future profession (The Department of Information Security)

The Department of Information Security in Bauman Moscow State Technical University was established in 1998 in order to develop the direction of training specialists in new, relevant areas of computer science.

The main scientific direction and field of training is the comprehensive provision of information security of automated systems. The safety of automated systems is the direction of science and technology, encompassing a combination

of software and hardware, cryptographic, technical and organizational-legal methods and means of ensuring information security in automated systems while processing, storing and transmitting it using modern information technologies.

Information security of automated systems covers a combination of software and hardware, technical and organizational and legal methods and means of ensuring information security in automated systems when processing, storing and transmitting it using modern information technologies.

Computer security covers the development of the principles of building and methods of software and hardware implementation of modern information security systems using cryptographic tools.

On September 1, 2005, a network security laboratory was set up. The laboratory is equipped with modern terminals provided by AMD Company. It provides laboratory work for students of junior courses, as well as pre-diploma practice. In addition, new methods of training are successfully introduced on the basis of the network security laboratory. Among them, there is a range of distance learning courses on various disciplines developed at the department.

Students get knowledge on:

- Organizational and legal issues of information security (IS);
- High-level programming in modern operating environments;
- System engineering and circuit design of IS equipment;
- Assembler programming of the latest hardware platforms;
- Mathematical aspects of information protection, cryptography, steganography, crypto and steganalysis;
- The newest protected network technologies of global, corporate and local purpose.

Учебное издание

Ражева Елизавета Сергеевна
Смелкова Елизавета Андреевна
Трошина Ольга Валерьевна

ENGLISH FOR COMPUTER INFORMATION SECURITY SPECIALISTS
АНГЛИЙСКИЙ ЯЗЫК ДЛЯ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебное пособие

для студентов 3 курса, обучающихся по специальности «Информационная безопасность», квалификация (степень) «инженер»

ИД № …… от ……
Подписано в печать 00.00.00. Формат 60х90 1/16. Бумага офсетная. Печать трафаретная. Усл.печ.л. 9,3. Тираж 100 экз. Заказ .