Contents

ВВЕДЕНИЕ

В основе данного учебно-методического пособия лежит современный предметно-языковой интегрированный подход к обучению профессиональному иноязычному дискурсу в высших учебных заведениях. В соответствии с данным подходом студенты не только овладевают своей специальностью посредством иностранного языка, но и развивают целевые языковые компетенции во всех видах профессиональной речевой деятельности (чтении, аудировании, письме, говорении и переводе).

Учебное пособие ставит своей целью формирование профессиональных компетенций, обучающихся через структурно-компонентное, системное изучение тематического языкового материала в сфере информационной безопасности на русском и английском языках. Владение иностранным языком в совокупности с базовыми знаниями в области обеспечения информационной безопасности является ключевым условием для подготовки высококвалифицированных специалистов, отвечающих современным требованиям федерального государственного образовательного стандарта и конкурентоспособных на российском и международном рынке труда. Высокий уровень владения иностранным языком - не только цель для студента, но и средство получения информации для приобретения новых знаний в области информационной безопасности.

Настоящее учебно-методическое пособие направлено на решение следующих задач:

1) совершенствование навыков чтения и перевода аутентичных текстов преимущественно научно-исследовательского и аналитического характера, отражающих современное состояние сферы информационной безопасности и вопросы борьбы с киберпреступностью в России, Великобритании и США;
2) развитие навыков устной речи, а также формирование умения выступать публично;
3) развитие навыков письма в ходе выполнения творческих письменных заданий (деловое письмо, эссе, резюме, доклад);
4) развитие навыков аудирования в процессе работы с аутентичными видео- и аудиоматериалами, содержащими актуальную информацию о киберпреступности и информационной безопасности;
5) активизацию самостоятельной работы студентов в условиях широкого применения систем дистанционного обучения и использования информационных технологий и ресурсов.

Данное пособие рекомендовано для студентов, магистрантов и аспирантов, специализирующихся в сферах обеспечения информационной и национальной безопасности.

Unit 1.
Introduction to Cybersecurity

LEAD IN

Work in pairs and explain how you understand this quotation:

"Passwords are like underwear: don't let people see it, change it very often, and you shouldn't share it with strangers"

by Chris Pirillo

KEY TERMS

cybersecurity	кибербезопасность
to secure	защищать, охранять, обезопасить
cyber attack	кибератака
to attack	атаковать, нападать
attacker	злоумышленник, взломщик, хакер
hacker	хакер, злоумышленник
cyber threat	киберугроза
cyber defence	киберзащита
unauthorized access	несанкционированный, неавторизованный доступ
breach	взлом, повреждение, утечка (данных)
damage	вред, ущерб, урон
to steal	красть, воровать
data	данные, сведения, информация
sensitive (files, information)	конфиденциальный, личный, связанный с важной/секретной информацией
to encrypt	шифровать, кодировать
malicious	злоумышленнный, вредоносный

software	программное обеспечение (ПО)
malware	вредоносное ПО
blackmail	шантаж, вымогательство; шантажировать
phishing	фишинг (получение обманом личных данных пользователей)
denial of service (DoS)	отказ в обслуживании
scam	интернет-мошенничество, скам
digital	цифровой, электронный
authentication	аутентификация, авторизация, проверка подлинности
password	пароль
privacy	конфиденциальность
private	личный, конфиденциальный
regulation	правило, закон, регулирование
to comply with	соблюдать, выполнять, соответствовать
legitimate	законный, легитимный
enhancement	улучшение, усиление

VOCABULARY

Exercise 1

a. What parts of speech are the following words?

Security, insecure, attack, attacker, unauthorized, effect, affect, authentication, regulation, transferable, privacy.

b. Identify suffixes and prefixes where possible and translate the words.

Exercise 2

Which word is odd?

to secure	to protect	to maintain	to defend
issue	cause	problem	question
approach	attack	intervention	violation
digital	technological	numerous	computerised

private	personal	sensible	confidential
to discourage	to affect	to influence	to change
criminal	hacker	attacker	fisher

Exercise 3

a. Match the words with similar meaning:

1) threat	a) important
2) sensitive	b) law
3) various	c) improvement
4) vital	d) menace
5) enhancement	e) sophisticated
6) regulation	f) confidential
7) complex	g) different

b. Match the words with opposite meaning:

1) secure	a) defence
2) public	b) offline
3) legitimate	c) reduction
4) attack	d) vulnerable
5) online	e) out of reach
6) available	f) private
7) increase	g) illegal

Exercise 4

Match the words to the definitions:

1) digital	a) a dishonest and illegal way of making money by tricking people
2) blackmail	b) to act according to an order, rule, or request
3) to encrypt	c) to take advantage of something or somebody
4) scam	d) using or relating to computers and the internet
5) to comply with	e) to be forced to do something

6) to be compelled	f) to put information into a secret code so that most people cannot read it
7) to exploit	g) to make threats to harm a person or organization if they do not do something you want

Exercise 5

a. Match the word combinations:

1) malicious	a) regulations
2) data	b) system
3) to collect	c) authentication
4) to comply with	d) code
5) computerized	e) access
6) multi-factor	f) protection
7) to gain	g) data

b. Complete the following sentences using the words and word combinations from the previous tasks:

1. The number of global cyber th_____ continues to increase each year.
2. According to special regulations companies are c_____ to use clear and simple language when collecting personal data.
3. These days attackers are using more s_____ techniques to target the systems.
4. Government, military, corporate and medical organizations collect and store enormous amount of d_____ on computers and other devices.
5. One of the ways to protect your devices is to use m_____ authentication.
6. As the sophistication of cyber attacks grow, companies and organizations need to take steps to protect their s_____ information.
7. Viruses are usually attached to clean files and infect them with m_____ code.

Exercise 6

You know that some words can differ in British and American English. Place each word in the correct column:

program, programme, computerised, computerized, defence, defense

British English	American English

Notes:

*In British English the word **programme** refers only to a broadcast on television or radio (television programme, radio programme) or things to be followed in a prescribed order (fitness programme), but **program** is often used in computing contexts.*

Exercise 7

Match the parts of the sentences and translate them into Russian:

1. Large companies often become	a) trust with customers and employees.
2. One computer could send another	b) significant fines for cybersecurity breaches.
3. Cybersecurity affects	c) the target of sophisticated cyber attacks.
4. It is important to have	d) instructions to delete everything on it.
5. Data protection laws mean organizations can face	e) the higher the risk of security vulnerabilities.
6. By not being secure on the Internet we risk	f) a different password for every website you visit.
7. The more you connect to digital assets	g) losing money or sensitive information.

Exercise 8

Translate the sentences from Russian into English using the words and word combinations from the previous tasks:

1. Цифровая трансформация общества приводит к тому, что все больше преступлений совершается онлайн.
2. Кибератака – это действия, которые нацелены на сбор конфиденциальной информации.

3. Это электронное письмо зашифровано, вам нужно ввести пароль, чтобы его прочитать.
4. Программное обеспечение для кибербезопасности – это любая компьютерная программа, обеспечивающая защиту вашей информации.
5. Хакеры получили доступ к аккаунту электронной почты Марии и отправили ее друзьям вредоносное ПО, чтобы украсть информацию об их банковских аккаунтах.
6. Эксперты в области кибербезопасности находят и анализируют новые угрозы, а также разрабатывают способы борьбы с ними.
7. Крупные корпорации могут быть уязвимы для шантажа компьютерных хакеров.

Exercise 9

Work in pairs. Discuss the questions:

1. Can you imagine our modern world without digital devices? Why?
2. Why is it important to protect data?
3. What kind of cyber threats can you think of?

READING I

Exercise 10

Read the text and give a short summary to answer the question in the title.

WHAT IS CYBERSECURITY?

Imagine an employee working with data at the corporate computer. In the background, the company's sensitive files are secretly accessed by a hacker. He steals confidential information and sells it to criminals who blackmail the company for profit. It may sound like a story out of a movie, but the truth is that it is common in today's online environment and can happen to any user, not just to companies and organizations.

The world of digital crime is vast and not limited to any particular platform accessible via the Internet. Although computers, smartphones and tablets all have some level of digital defence, each also has its "weak points" that hackers have learned to exploit. This is why cybersecurity has become a vital part of any sphere of modern life and there is an increased need for cybersecurity experts.

Let's have a closer look at what cybersecurity is. The word "cybersecurity" is made up of two words – cyber and security. The dictionary defines the word "cyber" as relating to computer or electronic communications, especially the Internet. And security is all about being safe or protected. So, cybersecurity is the practice employed to protect and secure computers, servers, networks, mobile devices, electronic systems, and data from being attacked. This term is used in a variety of contexts, from business to mobile computing. It can be divided into several categories: network security, application security, information security, and operational security.

Providing cybersecurity generally requires knowledge of potential threats such as viruses and other malicious objects. Here are some examples of the most common methods to gain control of computer systems:

- Malware – is malicious software. In other words, it is software that is created by a hacker or a cybercriminal to damage a legitimate user's computer (for example, trojans, spyware or ransomware);
- Phishing – is an attack with a seemingly legitimate-looking e-mail aiming to disclose sensitive information (for example, credit card data or passwords);
- Denial of Service (or DoS) – is an attack where hackers overload networks and servers with traffic so that computer systems are unable to keep up with legitimate needs. As a result, an organization cannot carry out vital functions.

Global cyber threats continue to evolve rapidly, with an increasing number of breaches each year. Therefore, learning about cybersecurity is more important than ever to develop secure software, identify and respond to cyber attacks and critically analyze digital evidence to solve and prevent crimes. And the most crucial part is that cybersecurity makes our lives much safer.

https://www.simplilearn.com/introduction-to-cyber-security-article
https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

Exercise 11

Decide if the statements are true or false. Correct the false statements.

STATEMENT	TRUE	FALSE
1. A cyber attack can happen to any user, not just to companies and organizations.		
2. The term 'cybersecurity' is used only in programming		
3. Cybersecurity includes network security, application security and mobile security.		

4. There are plenty of cyber threats such as malware, phishing, DoS, etc.
5. Phishing is software created by a hacker to cause harm to a legitimate user's computer.
6. Denial of Service is an attack where the main aim of hackers is to steal confidential information.
7. As the number of cybersecurity experts is increasing and they develop new ways to respond to cyber attacks, the number of breaches start decreasing each year.

Exercise 12

Find in the text the derivatives of the words:

access, employ, computer, crime, increase, security.

Exercise 13

Find in the text and translate sentences which contain:

Passive Voice and Degrees of Comparison.

Exercise 14

Finish the following sentences:

1. A hacker steals confidential information and sells it to criminals who…
2. The world of digital crime is vast and not limited to…
3. Cybersecurity has become a vital part of…
4. The dictionary defines the word "cyber" as relating to…
5. Cybersecurity is the practice employed to protect and secure…
6. Providing cybersecurity generally requires…
7. Phishing – is an attack with a seemingly legitimate-looking e-mail aiming to…

Exercise 15

Read the text and fill in the gaps with the words in the box:

increase	cybersecurity	protection	damages	private
networks	cyberattacks	reputation	reduce	

(1) _____ is important to every organization, no matter how big or how small. There are roughly 4,000 (2) _____ every day. One reason the rate of cybercrime continues to (3) _____ is because it is cheap, fast, and highly profitable compared to other types of crime. Cybercrime can cost organizations millions of dollars in (4) _____. It can also damage their (5) _____ and their ability to do business. When people don't feel that their information is being properly secured and kept (6) _____, they begin to lose trust in the product and the services. Securing user identities helps (7) _____ the risk of cybercrime to organizations and to individuals alike. As organizations evolve and grow over time, their (8) _____ and systems naturally get more complicated, and things may slip through the cracks. That requires the organizations to put robust security (9) _____ in place.

LISTENING I

Exercise 16

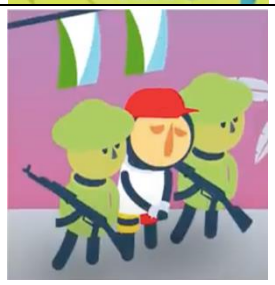
You are going to watch a video "A Cyber Privacy Parable" at https://www.youtube.com/watch?v=H0I7jQb37bo

a. BEFORE YOU WATCH. Answer the questions:

1. How often do you post things online?
2. Do you think it is dangerous to post pictures online? Why?
3. Do you think your passwords for different sites and social networks are secure? Why?

b. WHILE YOU WATCH. Make notes about the main events of Tim's story.

1) 	

2)		
3)		
4)		
5)		

c. AFTER YOU WATCH.

1) Using your notes in the exercise b retell Tim's story.

2) In pairs discuss the following questions:

1. Have you or your friends ever been hacked?
2. Who can store information that you post publicly?
3. Who can intercept your private communications?
4. Every year over ten million Americans have their identities stolen. Why do you think this number is so big? Why does it happen?
5. What can we do to protect ourselves online?

READING II

Exercise 17

Read the text.

CYBERSECURITY BASICS

With cyber threats and attacks overgrowing, cybersecurity remains one of the most concerning matters nowadays. Individuals, small businesses, and large organizations are all affected. Understanding and practicing cybersecurity basics can help to protect you and your business and reduce the risk of cyber attacks. All you have to do is to follow 5 simple rules:

1) Update your software

It is important to update your apps, web browsers, and operating systems. This will keep your defence system up to date and capable of protecting you from the newest cyber threats. It is better if you set updates to happen automatically.

2) Secure your files

Make sure you back up your important files offline (in an external hard drive or in the cloud). It will help you restore your device quickly in the event of data loss. Keep your paper files safe as well.

3) Require passwords

You should use strong passwords on all your laptops, tablets, and smartphones. Do not leave these devices unattended in public places such as, for example, cafes, trains or coworking because anyone can approach your device while you are gone.

4) Encrypt devices

It is also a good idea to encrypt devices and other media containing sensitive personal information. Encryption turns information into an illegible secret code making it gibberish to anyone without a password or a key, in case, for example, your device gets stolen.

5) Use multi-factor authentication

It is necessary to require multi-factor authentication when accessing areas of your network with sensitive information. This requires an extra step beyond logging in with a username and a password. For example, a temporary code on your smartphone or a key plugged into your computer, which makes stealing your information harder.

Following these rules is not difficult and may help you to ensure data protection and minimize the risk of cyber attacks.

https://www.ftc.gov/system/files/attachments/cybersecurity-small-business/cybersecuirty_sb_factsheets_all.pdf

Exercise 18

Answer the questions:

1. Why is it important to update your software?
2. In what case backing up important files offline can be helpful?
3. Why can it be unsafe to leave your devices unattended in public places?
4. What is encryption and why is it useful?
5. Why using multi-factor authentication makes stealing your information harder?

Exercise 19. Internet Activity

Group work. The class is divided into two groups (A and B). Each group reads and discuss an article:

Article A : https://www.ncsc.gov.uk/guidance/shopping-online-securely

Article B : https://www.cbc.ca/news/science/how-to-stay-safe-with-a-smartphone-1.2553592

After reading and discussing each group is supposed to make a list of

- **Group A: Top-5 things to shop online securely;**
- **Group B: Top-5 things to stay safe with a smartphone.**

Then each group shares with one another their knowledge on the topic.

LISTENING II

Exercise 20

You are going to watch a video "GDPR: What Is It and How Might It Affect You?" at https://www.youtube.com/watch?v=j6wwBqfSk-o

a. BEFORE YOU WATCH. Answer the questions:

1. What do you understand by personal data?

2. Do you think government should protect your personal data? Why?
3. Do you know any laws or regulations that help to protect people's data?

b. WHILE YOU WATCH. Fill in the gaps:

The General Data (1)_____ Regulation or GDPR – as you've likely heard it called. It goes into (2)_____ on May 25th, and it could (3)_____ you no matter where you are or where you live.

So, what is GDPR? It (4)_____ Europe's already strict (5)_____ about what companies can do with people's (6)_____. It gives you more (7)_____ over how your data is (8)_____ and used and forces companies to (9)_____ everything that they do with it. While GDPR is European Union (10)_____ it has a huge effect on businesses outside the EU including the US.

Why was GDPR introduced? Because the old laws were (11)_____ before smartphones started (12)_____ massive amounts of (13)_____ information for companies like Google and Facebook. GDPR gives organizations (14)_____ on what they can and can't do with personal data. <…>

What is considered personal data under GDPR? Any data that can (15)_____ you: that's your name, phone number or (16)_____, but the law also includes things like your IP address or (17)_____ data. <…>

How will it affect you? One way is that you will often have to (18)_____ in to letting a company use your data. This means fewer (19)_____ boxes and firms are (20)_____ to use clear and simple language.

Do people have the "right to be forgotten"? Yes, people can (21)_____ to have their data (22)_____. <…> However, the right to be forgotten is not (23)_____ and certain conditions apply.

Why is GDPR a concern for non-EU countries? Because many (24)_____ collect or use EU residents' data. They also use companies (25)_____ in the EU for services and (26)_____ data.

What happens if a firm doesn't comply with GDPR? The (27)_____ could be up to 20 million euros or 4% of annual (28)_____ whichever is larger.

c. AFTER YOU WATCH. Answer the questions:

1. What does GDPR stand for?
2. What does GDPR do?
3. Does GDPR affect business outside the EU? Why?
4. What is the "right to be forgotten"?
5. How does GDPR affect users?

GRAMMAR

Exercise 21

a. Study and compare the ACTIVE VOICE and PASSIVE VOICE tables (see GRAMMAR REFERENCE pp. 170-171).

b. Choose the correct form (Active or Passive). Translate the sentences.

1. An unauthorized version of the software *is selling / is being sold* abroad.
2. If you *have received / have been received* an email which you're not quite sure about, don't click on any links.
3. The company also *announced / was announced* enhancements to three of its online databases.
4. We have not had any contact with the hackers and no ransom ask *has made / has been made*.
5. According to the GDPR businesses *require / are required* to protect against unauthorised or unlawful use of the personal data.
6. Campaigners *will protest / will be protested* if the sensitive medical information *releases / is released*.
7. Special tools and technologies *implemented / were implemented* to detect any change or a breach in the data.

c. Open the brackets using Active or Passive Voice, mind the grammar tense:

1. The company's automated systems _____ (to detect) a cyber attack.
2. Informing people whose personal data _____ (to stole) _____ (to do) through phone calls, public announcements, and letters.
3. Security programs _____ (to continue) to evolve new defences as cyber-security professionals _____ (to identify) new threats.
4. When buying things online you _____ (to give) options to pay through your debit or credit card.
5. We _____ (to make) a lot of enhancements to the software and it _____ (to strengthen) system security.
6. The email _____ (to encrypt), so you will need to enter a password to read it.
7. With the development of modern technologies shoppers _____ (to get) used to buying online.

d. Translate the sentences from Russian into English:

1. Фишинговые электронные письма могут содержать ссылки на веб-сайты, которые заражены вредоносным ПО.
2. Убедитесь, что ваши действительно важные учетные записи защищены надежными паролями, которые вы больше нигде не используете.
3. Защищенные веб-сайты сообщат вам, что передача данных зашифрована, и ваш браузер отобразит символ, подтверждающий это.
4. Небольшие организации из определенных секторов в Великобритании будут приглашены принять участие в специальной программе по кибербезопасности.
5. Система подверглась кибератаке, но никакие данные не были удалены при взломе.

Exercise 22

a. Study the DEGREES OF COMPARISON table (see GRAMMAR REFERENCE p. 172).

b. Complete the sentences with a comparative adjective:

1. This year the number of data breaches is _____ than it was last year. (big)
2. Updates usually contain changes that will make your device _____. (secure)
3. The more you connect to digital assets, the _____ the risk of security vulnerabilities for your sensitive data. (high)
4. Learning about cybersecurity is _____ than ever. (important)
5. Modern computers are much _____ than the early ones. (fast)
6. Some sectors are at _____ risk of cyber attack and _____ to access than others. (great, easy)
7. Malware can be far _____ if it isn't identified and removed. (dangerous)

c. Complete the sentences with a superlative adjective:

1. _____ passwords are _____ than eight characters and usually contain a variety of characters, numbers, and special symbols. (strong, long)
2. Clicking on that suspicious link was _____ mistake in my life. (stupid)
3. Cloud backups are now _____ solution to cope with data loss, accidental deletion, or cyber attacks. (trusted)
4. What is _____ way to steal somebody's confidential information? (easy)
5. To stay safe online, it's important to know some of _____ cyber security terms and definitions. (common)

6. The business has invested heavily in _____ technology. (late)
7. The problems of security and privacy relating to online trading represent _____ barrier to e-commerce. (significant)

d. Translate the sentences from Russian into English:

1. Даже самые лучшие и самые сильные компании могут столкнуться с проблемами кибербезопасности.
2. Поскольку организации развиваются и растут со временем, их сети и системы становятся более сложными.
3. Пароли, состоящие только из цифр, хуже паролей, которые содержат разнообразные буквы, цифры и специальные знаки.
4. Надежное ПО является одним из самых эффективных способов защиты от киберугроз.
5. В настоящее время кибератаки становятся все более инновационными.

SPEAKING

Exercise 23

a. Read the e-mail. What would your reaction be if you got an e-mail like this? Why?

Subject: Businness opportunity
Dear friend, I know that you will be surprised by this message. My name is Rose Agot, and I work at the Transnational Bank in Nairobi, Kenya. My parents have died two months ago and left $5.3 millions in their acount. I am needing to transfer this money out of Kenya and I would like to ask you for help. I can to transfer the entire amount of money to you in Russia, and then you can keep 15% of the money ($795,000) as a reward for you help and transfer the rest to the account in Switzerland. It should be simple and won't take a lot of time. I would be really grateful if you agree to do this for me, becase I want to keep my parents' money safe for my family. Please reply to this e-mail as soon as possible. I hope organize everything by the end of the week. Thank you in advance. Rose Agot

b. Scam e-mails often contain a lot of spelling and grammar mistakes. Correct all the highlighted mistakes.

c. Have you ever received e-mails like this? Have you or your family members / friends ever been the victim of a scam? Discuss with the class.

d. Read the statement:

Being scammed is always your fault.

In pairs, discuss whether you agree or disagree with this statement. Explain why.

Use the following phrases to help you:

Agreeing	*Disagreeing*
I agree with you / the statement / the idea, etc.).	(I'm afraid) I don't agree with / I disagree with you / the statement / the idea, etc.
Yes, you are / the statement is (quite) right.	You are wrong there. / The statement is wrong.
That's true / correct.	That isn't true / correct.
I totally agree!	I totally disagree!
Exactly!	That's not right!
I really think so!	I don't think so!
Of course!	Of course not!
Certainly!	Certainly not!
I couldn't agree more.	I believe not.
That's a good point.	I'm not sure about that.
That's exactly how I feel.	That's not always true.
I agree with you 100 percent.	I'd say the exact opposite.

READING III

Exercise 24

Read the text and match the questions (1–5) to the paragraphs (A–E) that contain the answers:

1	2	3	4	5

1. How confident is ICRC that the hackers are no longer in their systems?

2. What went wrong with ICRC's defences?
3. What happened?
4. What is the organization doing to prevent this from happening again?
5. What made this cyber attack complex and targeted?

CYBER ATTACK ON ICRC[1]

A. In January 2022 the ICRC discovered that servers hosting personal data for over 515,000 people (names, locations, and contact information) worldwide had been hacked in a sophisticated cyber attack. As a humanitarian organization the ICRC considers its duty to share with its partners and the people it serves all available information on this hack.

B. The hackers have used considerable resources to gain access to the systems of the ICRC. They made use of tactics that most detection tools would not detect. These are the facts that reveal the sophisticated and targeted nature of the attack:
   - The set of hacking tools that was used by the hackers is very specific. It is out of reach to other actors and is not available publicly.
   - The attacker managed to hide and protect their malicious programs which is only possible for actors with an extra high level of skills.
   - Most of the malicious files were specifically crafted to bypass the organization's anti-malware solutions.

C. Every year the ICRC implement a great number of patches across all their systems. Unfortunately, a critical patch was not applied in time before the hack took place. Although the organization has a multi-level cyber defence system, its vulnerability management processes and tools did not stop this breach.

D. As soon as they realized that the servers had been hacked, they took them offline. The ICRC segment its systems and use advanced tools to continuously monitor its entire environment for signs of malicious activity, that is why this incident did not affect any other servers.

E. After the attack the cyber defence systems have been relaunched with security enhancements that include advanced threat detection solution and new two-factor authentication process. The organization continue to closely monitor its systems and make appropriate security enhancements. Now the ICRC is also working with its partners in humanitarian field to spread information about the importance of protecting humanitarian organizations both online and offline.

https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know

Notes:

[1]*ICRC – International Committee of the Red Cross, an organization that helps people affected by armed conflict and promotes respect for international humanitarian law*

Exercise 25

Match the words and phrases with their Russian equivalents:

1) to be out of reach	a) внедрять, применять
2) to bypass	b) взлом, повреждение, утечка (данных)
3) to implement	c) система киберзащиты
4) patch	d) быть недоступным, вне досягаемости
5) breach	e) усиление, укрепление безопасности (меры по усилению безопасности)
6) cyber defence system	f) обойти, миновать
7) security enhancements	g) ПО для оперативного исправления ошибки в программе, патч («заплата»)

Exercise 26

Make a summary of the text you have read. Share information with other students.

WRITING

Exercise 27

a. Read and translate the e-mail:

From: s_anderson@bestcompany.com **To: j_williams@bestcompany.com** **Subject: Employee training**
Dear Mr. Williams, I am writing to invite you and the employees of your department to a cybersecurity training that will take place at 3 p.m. on 17 October. I would like to request a list of employees that are going to attend this training. However, some members of the staff will have to stay in the workplace to process

incoming requests from clients. There will be an additional training for them next month. I look forward to hearing from you. Yours sincerely, Susan Anderson

b. Look at the phrases in the first column and find their formal equivalents in the text (exercise a):

Informal	**Formal**
Hi / Dear [first name]	
I'm writing	
I'd like	
But	
Hope to hear from you soon.	
Best wishes / Love	

c. Study the essential information about writing formal e-mails:

Formal e-mails are usually sent to people in an official position or people we don't know. They include five parts:

1. **Formal greeting** *(Dear Mr/Mrs/Ms [surname] / Dear Sir/Madam / To whom it may concern)*
2. **Introduction** with opening remarks and the reason for writing (*I am writing to… / I am writing in reference to…)*
3. **Main body** varies according to the function of what you need to communicate
4. **Conclusion** with closing remarks *(I look forward to hearing from you / Thank you in advance)*
5. **Formal ending:** *Best regards,* / *Kind regards, / Yours sincerely,* (if you began the email with 'Dear Mr/Mrs/Ms [surname]) / *Yours faithfully,* (if you began the email with 'Dear Sir/Madam' – you don't know the person's name) + [your name and surname]

There are a few characteristics of **formal style** that you should remember writing a formal e-mail:

- Stick to formal expressions and advanced vocabulary
- Make longer sentences
- Do not forget about formal linking words
- Use full verb forms
- Try to use the passive forms where it is possible

d. Write a formal e-mail using the information from the exercises b and c:

You received an e-mail from your company's partner, but it looks very suspicious: it contains a very generous offer and a link. You do not know what to do, so you decide to write an e-mail to the IT manager explaining your situation. Describe the problem and ask for further instructions.

TRANSLATION PRACTICE

Exercise 28

Translate the text into Russian.

NCSC[1] CEO[2] MEETS WITH CYBER SECURITY LEADERS IN INDIA

Lindy Cameron CEO of the NCSC made an official visit to India this week for a series of meeting with government officials, businesses, and academics to discuss the shared opportunities and challenges that India and the UK face in cyberspace.

She visited the capital New Delhi and the India's IT capital Bangalore and had talks with key Indian cyber security partners – National Cyber Security Coordinator, Rajesh Pant, and the Secretary of the Ministry of Electronics and Information Technology (MEITY), Shri Alkesh Sharma.

Leaders from the Karnataka Police Department shared with Lindy Cameron their thoughts on how to collaborate effectively with law enforcement. She also met Rolls Royce executives who described their ways of businesses operating in India's cyber security ecosystem. Moreover, NCSC CEO visited the International Institute of Information Technology, Bangalore, where she had an interactive Q&A[3] session with their students.

All in all, this was the first time CEO of the NCSC visited India since the release of the India–UK cyber statement last year, which reaffirmed the countries' shared commitment to promoting a stable, secure, and peaceful cyberspace.

Notes:

[1]*NCSC – National Cyber Security Center (UK)*

[2]*CEO – Chief Executive Officer*

[3]*Q&A – Question and Answer*

https://www.ncsc.gov.uk/news/ncsc-ceo-meets-with-cyber-security-leaders-in-india

TEST 1.
INTRODUCTION TO CYBERSECURITY

Choose the correct answer to complete the sentences:

1. The practice employed to protect and secure computers, servers, networks, mobile devices, electronic systems, and data from being attacked is called…

a) cyber defence;
b) authentication;
c) cybersecurity;
d) encryption.

2. An attack where hackers overload networks and servers with traffic so that computer systems are unable to keep up with legitimate needs is called…

a) phishing;
b) denial of service (DoS);
c) malware;
d) blackmail.

3. … is an attack with a seemingly legitimate-looking e-mail aiming to disclose sensitive information.

a) phishing;
b) denial of service (DoS);
c) malware;
d) blackmail.

4. GDPR stands for…

a) General Data Privacy Rule;
b) General Data Prevention Rule;
c) General Data Privacy Regulation;
d) General Data Protection Regulation.

5. When Tim … his photo to the Internet, it … in a few places.

a) uploaded; were stored;
b) was uploaded; stored;
c) uploaded; was stored;
d) was uploaded; were stored.

6. Jane … online when her credit card details ... .
a) was shopping; were stolen;
b) were shopping; were stolen;
c) was shopping; was stolen;
d) was shopping; had been stolen.

7. If you update your software, it will keep your defence system up to date and capable of protecting you from the … cyber threats.
a) more new;
b) most new;
c) newer;
d) newest.

8. The … part of cybersecurity is that it makes our lives much … .
a) crucialest, safer;
b) more crucial, more safe;
c) most crucial, safer;
d) most crucial, safest.

9. To… means to put information into a secret code so that most people cannot read it.
a) exploit;
b) encrypt;
c) comply;
d) secure.

10. … means intended to cause harm to a computer system or to steal sensitive information.
a) Digital;
b) Legitimate;
c) Malicious;
d) Computerized.

11. As soon as the company realized that the servers … , they … them offline.
a) hacked, took;
b) are hacked, take;
c) had been hacked, took;

d) had been hacked, were taken.

12. People … to lose trust in the company if they don't feel that their information … properly.

a) began, secured;
b) begin, is being secured;
c) begin, is secure;
d) began, is been secured.

13. Using secure software is one of the … ways to protect your computer from cyber threats.

a) good;
b) most good;
c) goodest;
d) best.

14. Multi-factor … is a user verification technology that requires more than one type of user validation.

a) password;
b) regulation;
c) authentication;
d) identification.

15. Large organizations can be vulnerable to … demands by computer hackers.

a) blackmail;
b) scam;
c) criminal;
d) online.

Unit 2.
Basics of Cybercrime

LEAD-IN

Work in pairs and explain how you understand this quotation:

"If you put a key under the mat for the cops, a burglar can find it, too. Criminals are using every technology tool at their disposal to hack into people's accounts. If they know there's a key hidden somewhere, they won't stop until they find it"

by Tim Cook

How would you complete the saying?

"_____ is the greatest threat to every company in the world"

by Ginni Rommety

KEY TERMS

illegal	незаконный
to commit a crime	совершить преступление
criminal (n) **criminal (adj)**	преступник (сущ.) уголовный (прил.)
invasion of privacy	вмешательство в личную жизнь
to locate	определять точное местонахождение
to promote	продвигать
to revolve around	быть так или иначе связанным с
to implement laws	реализовывать/вводить в действие законы
to pass laws	принимать законы
victim	потерпевший, пострадавший, жертва
to deal with	иметь дело/ заниматься чем-либо
to withdraw	снимать со счета
to make purchases	делать покупки
to eliminate	устранять
identity theft	кража персональных данных

fraud	мошенничество
harassment	харассмент, домогательство, преследование
cyber stalking	киберпреследование – использование интернета для преследования или домогательств человека, группы людей или организации
gambling	игра на деньги/игра в азартные игры
web jacking	незаконное получение контроля над веб-сайтом путем захвата домена
vulnerable	уязвимый, незащищенный

Exercise 29

a. What parts of speech are the following words?

Illegal, in-house, revolve, appropriation, proprietary, unauthorized, use, invasion, implement, transferring, goods, data, criminal, specifically.

b. Identify suffixes, prefixes and translate the words:

Unauthorized, information, illegally, appropriation, impossible, unsolicited, specifically, minimize, issuance, simultaneously.

Exercise 30

Which word is odd?

illegal	legitimate	unlawful	criminal	illicit
criminal	offender	victim	wrongdoer	perpetrator
abandon	support	look after	oversee	take care of
eliminate	clear	remove	expel	maintain
stolen	appropriated	illegal	robbed	purchased
access	denial	entrance	acceptance	permission

Exercise 31

a. Match the words with similar meaning:

1) offence	a) money
2) law	b) unsolicited email
3) goods	c) act
4) funds	d) information
5) spam	e) products
6) network	f) crime
7) data	g) web

b. Match the words with opposite meaning:

1) private	a) purchase
2) implement	b) deposit
3) steal	c) profit
4) withdraw	d) public
5) assets	e) exactly
6) debt	f) liabilities
7) loosely	g) cancel

Exercise 32

a. Match the words to the definitions:

1) to generate	a) to be centered or focused upon
2) to revolve	b) to do something illegal
3) to deal with	c) to support or actively encourage
4) to locate	d) to be concerned with
5) to provide	e) to discover the whereabouts of
6) to implement	f) to produce or create something
7) to promote	g) to put smth. into effect.
8) to commit	h) to give someone smth. that they need

Exercise 33

a. Match the word combinations:

1) to implement	a) illegally obtained data
2) to pass	b) cybercrimes
3) to use	c) stolen funds
4) to deal with	d) laws
5) to steal	e) purchases

6) to make	f) financial information
7) to transfer	g) cybercrime law
8) to commit	h) huge debts

b. Complete the following sentences using the words and word combinations from the previous tasks:

1. Company was able freeze the account to which the (1)_____were _____.
2. This helps better determine how to (2)_____ in the cyber environment.
3. The (3)_____ was _____ in early 2006.
4. Last week China Central Television (CCT) claimed that Windows (4)_____ from computers, and transmitted it to the U.S.
5. The study showed that almost all European online buyers (96%) at least once (5)_____ in multi-brand online stores.
6. Suspects of online crime often (6)_____to defraud the public and make money.
7. During the election campaign of 2016, Republican candidate Trump assured everyone that he would (7)_____ and liquidate them within eight years.
8. Cybercriminals can access web servers and (8)_____ such as hacking websites or transferring stolen money.

c. Translate these sentences from Russian into English using the words and word combinations from the previous tasks:

1. Преступники могут совершать киберпреступления при помощи средств, не требующих глубоких технических знаний.
2. Полиция обнаружила финансовую документацию, подтверждающую незаконное перечисление похищенных средств через популярные банковские системы.
3. Сегодня, благодаря защищенным серверам, клиенты могут легко делать покупки онлайн.
4. Существуют специализированные вредоносные программы, предназначенные для хищения финансовой информации, так называемые банковские троянцы.
5. Британский парламент принял закон, совершенствующий систему защиты персональных данных.
6. Полиция подтвердила, что мошенники использовали незаконно полученные данные.

7. Для более эффективного исполнения законов необходимо совершенно четкое разделение исполнительной и судебной ветвей власти.
8. Может ли GPS мониторинг считаться вмешательством в личную жизнь?
9. Приложение позволяет проверять баланс вашего счета, просматривать транзакции и снимать средства.
10. Несмотря на принятые законодательные меры, доля спама в почтовом трафике продолжает расти.

Exercise 34

Match the parts of the sentences:

1. Law enforcement agencies around the world	a) having to deal with huge debts.
2. Many countries are beginning to implement laws	b) and make purchases using the stolen data.
3. This leaves the victim in the position of	c) cooperate in an effort to provide a true picture of cybercrime.
4. Cybercrime can also involve	d) that make spamming a criminal act.
5. Criminals can steal financial information	e) transferring the stolen funds through a variety of accounts.
6. Criminals withdraw funds from company reserves,	f) illegal access to company information.
7. Nations have passed cybercrime law packages	g) in an attempt to minimize the incidence of cybercrime.

Exercise 35

Work in pairs. Discuss the questions:

1. What is cybercrime?
2. What cybercrimes do you know?
3. What does cybercrime involve?
4. Have you ever faced with cybercrime?

READING I

Exercise 36

Read the text and name all the forms of cybercrimes.

WHAT IS CYBERCRIME?

A cybercrime is defined as any type of illegal activity committed over the Internet, a private or public network, or an in-house computer system. While many forms of cyber offences revolve around the appropriation of proprietary information for unauthorized use, other examples are focused more on an invasion of privacy. As a growing problem around the world, many countries are beginning to implement laws and other regulatory mechanisms in an attempt to minimize the incidence of cybercrime.

One speaks about electronic crimes when using illegally obtained data (e.g. credit card number), the criminal opens accounts, charges a wide range of goods and services, and then abandons the accounts. This leaves the victim in the position of having to deal with huge debts that he or she did not generate.

Cybercrime can also involve illegal access to company information. Just as with individuals, criminals can steal financial information and make purchases using the data, withdraw funds from company reserves, transferring the stolen funds through a variety of accounts and making it virtually impossible to locate the stolen assets.

In many countries around the world, nations have passed cybercrime law packages that make spamming a criminal act. Spam is loosely defined as unsolicited emails that are simultaneously sent to thousands or even millions of email accounts. As the problem grows, more politicians promote the idea of some sort of national or international cybercrime act that would specifically address the use of spam and either limit or eliminate the practice altogether.

Obtaining authoritative cybercrime statistics is not as easy as it would seem. Some incidents of electronic crime go unreported. If police knew about all cybercrime cases, they would be able to provide full statistics of this matter. However many law

enforcement agencies around the world cooperate in an effort to provide a true picture of cybercrime.

https://www.easytechjunkie.com/what-is-cybercrime.htm

Exercise 37

Decide if the statements are true or false. Correct the false statements.

STATEMENT	**TRUE**	**FALSE**
1. Generally, cybercrime is broadly described as any kind of legal action via the Internet, a private or public network, or an internal computer system.		
2. Cybercrimes range from misappropriation of proprietary information for unauthorized use to privacy invasion.		
3. Many nations are enacting laws and regulations in order to reduce cybercrime.		
4. Using illegally obtained data, cybercriminals open accounts, purchase goods and services, and the victims of the crime have to repay debts.		
5. Cybercrime does not extend to unauthorized access to business information.		
6. Many states have enacted cybercrime laws focusing on the use of spam, limiting or eliminating this practice altogether.		
7. Law enforcement agencies around the world cooperate in order to prevent, and provide full statistics of cybercrimes.		

Exercise 38

Find in the text the derivatives of the words: enforce, legal, spam, authorize, report, define, crime, property, invade, implementation, steal.

Exercise 39

Find in the text and translate sentences that contain:

Passive Voice, Modal verbs and Conditionals.

Exercise 40

Finish the following sentences:

1. Cybercrimes are generally defined as …
2. One speaks about electronic crimes when using illegally obtained data, the criminal …
3. Cybercrime can also involve …
4. Criminals can …
5. Nations have passed …
6. Spam is defined as …
7. Many law enforcement agencies around the world…

Exercise 41

Look through the short articles about cybercrime-related matters and complete them with the words in the box:

Hacking	Identity theft	Phishing	Cyber fraud
Intellectual property theft	Spamming		

1. ____ is the crime committed via a computer with the intent to corrupt another individual's personal and financial information stored online. It is the most common type of fraud and individuals and organizations need to be attentive and protect their information from fraudsters.
2. ____ is the use of electronic messaging systems like e-mails and other digital delivery systems and broadcast media to send unwanted bulk messages indiscriminately. The term ____ is also applied to other media like in internet forums, instant messaging, and mobile text messaging, and television advertising.
3. ____ is a type of online fraud that involves tricking people into providing sensitive information, such as passwords or credit card numbers, by masquerading as a

trustworthy source. _____ can be done through email, social media or malicious websites.

4. _____ is the act of identifying and then exploiting weaknesses in a computer system or network, usually to gain unauthorized access to personal or organizational data. _____ is not always a malicious activity, but the term has mostly negative connotations due to its association with cybercrime.

5. ____ is one someone steals an idea, creative expression, or invention from an individual or a company. IP theft can refer to someone stealing patents, copyrights, trademarks, or trade secrets. This includes names, logos, symbols, inventions, client lists, and more.

6. _____is the crime of obtaining the personal or financial information of another person to use their identity to commit fraud, such as making unauthorized transactions or purchases. Identity theft is committed in many different ways and its victims are typically left with damage to their credit, finance, and reputation.

Exercise 42

Read the text and match headings to the paragraphs:

CHARACTERISTICS OF CYBER CRIME

1. People with specialized knowledge	a. The geographical boundaries in cyberspace have been eliminated. A cybercriminal can commit a crime from anywhere in the world to another corner of the globe. For example, a North Korean hacker can access a United States-based computer system.
2. Virtual World	b. Collecting evidence of cybercrime and trying to prove it in court is a very complicated task. While committing a cybercrime, the offender invokes the jurisdiction of more than one country and at the same time, he lives in a safe place where it is impossible to trace him.
3. Collection of Evidence	c. Cybercrime concept is very different from traditional crime. This crime has also gained considerable attention compared to traditional crime due to the development of Internet technology. For this reason, it is necessary to examine the specifics of cybercrime.
4. Magnitude of cybercrime	d. Cybercrimes can only be committed through the technology, thus to commit this kind of crime one has to be very skilled in

	internet and computers and internet to commit such a crime. The people who have committed cybercrime are well educated and have deep understanding of the usability of internet, and that has made work of police machinery very difficult to tackle the perpetrators of cybercrime.
5. The Concept of cybercrime	e. The consequences of cybercrime go far beyond the economic costs. It also undermines the trust of Internet users and causes reputational damage to service providers. Cyber-attacks increase cross-national tensions because governments and critical infrastructure are becoming the targets. In spite of all this, however, there are still global laws, rules, and regulations to prevent cybercrime.
6. Geographical challenges	f. Cybercrime is committed in cyberspace, and the offender committing the crime is not physically located in cyberspace. Everything the perpetrator does while committing the crime is taking place online.

https://lawpage.in/cyber_laws/crime/characteristics

Exercise 43

Answer the questions:

1. What is the difference between conventional crime and cybercrime?
2. How can you characterize cybercriminals?
3. Can cybercrimes be committed in the jurisdiction without the criminal being physically present in it?
4. Everything the cybercriminal does while committing the crime is taking place online, is not it?
5. Is it difficult to collect evidence of cybercrime?
6. Why is the damage caused by cybercrime tremendous?

GRAMMAR

Exercise 44

Study grammar rules on the use of Conditionals (see GRAMMAR REFERENCE pp. 172-174). Read and translate the sentences and determine the type (0-III).

1. If he had learned English at school, he would not have had problems with programming.
2. If you have evidence, you can go to court.
3. If you commit cybercrime, you will be punished.
4. If you steal music or movies, you break the law.
5. If you provide us with personal details about yourself, we will not pass that information to any other third party unless required to do so by law.
6. We would have ordered the new computer if they had delivered it immediately.
7. If I knew his e-mail address, I could contact him.
8. I would have agreed with the contract if I had had enough time to think it over.
9. What would you do if your personal data were stolen?

Exercise 45

Underline the correct form to make conditional sentences.

1. If she *will graduate/graduates* successfully, she will find employment with an IT company in Moscow.
2. These topics *will be/would be* especially useful to you if you are new to cybersecurity.
3. If you *are/were* a lawmaker, what kind of law would you implement and why?
4. If your financial information had been stolen from the vendor, your money *would have been/will be* at risk.
5. Your credit card protects you from any serious financial harm even if your card number *is lost/was lost* or *is stolen/was stolen*.
6. The evidence *may not/might not* be useful if it is obtained illegally.
7. He would have been on time for the job interview if he *had left/left* the house in time.
8. If my card was stolen, I *would/will* immediately report its stolen status to the credit card company and local police.

Exercise 46

Open the brackets using the correct form of the verb in the sentences below.

1. If the telephone (*to steal*), then a telephone theft claim to a police should be written.
2. I (*to attend*) the IT security conference if I had been aware of it.
3. If I (*to install*) anti-virus program, my computer would not have been hacked.

4. If your intellectual property is used illegally, the specialists of our law firm (*to help*) you to deal with this problem.
5. If I were you, I (*to plan*) my distance work very carefully in advance.
6. If you (*to spend*) the whole week preparing for the IT law exam, you will pass it well.
7. If someone (*to steal*) your password, you can just change it.
8. If I don't have time, I (*to make*) purchases online.

Exercise 47

Complete the sentences.

1. The cyber criminals can steal confidential information if …
2. If you make purchases at an unsecured website,…
3. Any person with a computer will become a software pirate if …
4. If I had known about this type of cyber fraud,…
5. Your computer would not have been hacked if…
6. If I were you, I…
7. If you don't have a good antivirus program,…
8. I will be happy if…
9. You could save time and money if..
10. John would not have committed cyber offence if

Exercise 48

Prepositions. Fill in the gaps where necessary with the prepositions.

of (2)	to (6)	in (2)	with	through
	for (2)	of	into	

Identity theft is the crime (1) _ obtaining the personal or financial information (2)_ another person (3)_ use their identity (4)_ commit fraud, such as making unauthorized transactions or purchases. Identity theft is committed (5)_ many different ways and its victims are typically left (6)_ damage (7)_ their credit, finances, and reputation.

Identity theft can be committed (8)_ many different ways. Some identity thieves sift (9)__ trash bins looking (10)_bank account and credit card statements.
Identity thieves increasingly use computer technology (11)_ obtain other people's personal information (12)_ identity fraud. (13)_ find such information, they may search

the hard drives (14)_stolen or discarded computers; hack (15)_computers or computer networks; access computer-based public records; use information-gathering malware (16)_infect computers.

Exercise 49

Crime idioms

a. Study information in the table:

Idiom	**Meaning**
1) to cover someone's tracks	to hide or to get rid of incriminating evidence
2) to catch someone red-handed	to discover someone in the act of wrongdoing
3) to do time / to be behind bars	to serve time in prison
4) not to have a leg to stand on	not to have sufficient evidence to prove something
5) to face the music	to accept the responsibility and punishment for something
6) to turn a blind eye to something	to ignore something that is wrong, immoral, or illegal

b. Complete the sentences with the idiom from the table above:

1. Both her parents were _____, so she was raised by her aunt.
2. The government should not _____ to cybercrime.
3. It's time to pardon Mr. Snowden and bring him home, not to _____ but to work for the security and privacy of all of us.
4. The lawyer of the other side doesn't _____.
5. I can't imagine how difficult it must be _____ for decades.
6. Unless we _____ properly, the police are sure to find us.
7. If the police had arrived five minutes earlier, all the offenders would have been _____.

c) Think of your own sentences with crime idioms.

READING II

Exercise 50

a. Match the terms with their definitions.

1) harassment	a) the repeated use of electronic communications to harass or frighten someone, for example by sending threatening emails
2) spoofing	b) the activity of betting money, for example in a game
3) cyber stalking	c) aggressive pressure or intimidation
4) defamation	d) the practice of registering names, especially well-known company or brand names, as internet domains, in the hope of reselling them at a profit
5) cheating	e) illegally seeking control of a website by taking over a domain
6) gambling	f) software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system
7) fraud	g) the legal right to control the production and selling of a book, play, film, photograph, or piece of music
8) cybersquatting	h) a large amount of money that is demanded in exchange for someone or something
9) malware	i) accessing a computer without proper authorization and gaining financial information from any protected computer
10) cyber trespassing	j) corresponds to theft or interception of data by capturing the network traffic
11) copyright	k) behaving in a dishonest way
12) ransom	l) the fraudster uses forged documents in order to gain access to information or materials they should not have access to
13) sniffing	m) the action of damaging good reputation of someone
14) denial of service attacks	n) the crime of getting money by deceiving people
15) web-jacking	o) occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor

16) forgery

p) a cybercriminal activity where someone pretends to be a colleague, or other trusted contact for stealing personal data or money

b. Find 14 words from a.

K T G U Y F F R I L K F E D O
N K N I T N T H O B E R C G O
S A I N N O M H A G A B F M Y
T T T A K I O E A B Y T G R I
R A T B F T S G N D G M G G C
A C A Q A A N I U O N N N A Y
N O U F H M A A R T I I I M B
A P Q F A A R Y F F T L K B E
H Y S I R F N R F U A F C L R
K R R R A E G I T F E A A I S
M I E S S D N N R I H T J N T
G G B I S S I G A O C Y B G A
D H Y S M T F I F A R R E W L
R T C H E A O A F N H E W C K
R O C I N P O A I M G G S A I
F E F I T G P G C D A R R A N
I M S E N M S G K P B O T I G
U O G K G R S U I A A F T F I
I M N T L N I F N F W N U F T
P R I I G A F O G I C E R G A

Exercise 51

Read the text and match headings to the paragraphs:

LEGAL CLASSIFICATION OF CYBERCRIME

1. Introduction	a. Generally, ordinary individuals are the most vulnerable targets of cybercriminals. This is due to various reasons like lack of information, guidance, and cyber-security. The goal is to exploit human weakness like greed and naivety. The potential harm of such a crime to humanity is severe. Few of the popular cybercrimes against persons include child-pornography, violation of privacy, harassment of a person through e-mail spoofing, hacking, cyber stalking, defamation, cheating, fraud, credit card frauds, gambling etc.
2. Cybercrime against individuals	b. The cyber crimes mainly targeting individuals may help cybercriminals get only a small amount of ransom, depending on the financial status of the targeted individuals. On the other hand, cyber-attacking large companies or organizations can help them get their hands on extremely confidential data of both private and public institutions and entities. Cyber-attacks on organizations are generally launched on a large scale to get a lump sum amount of ransom. Since such attacks drastically damage the companies' daily operations, most companies try to resolve them as fast as possible and to catch the offenders red-handed. The following are the kinds of cyber crimes launched targeting organizations. One of the distinct cybercrimes against government and related organizations is cyber terrorism. Cybercrime against organization mainly includes unauthorized access of computer, password sniffing, denial of service attacks, malware attacks, industrial espionage, forgery, web-jacking etc.
3. Cybercrime against property	c. Apart from the cyber crimes committed targeting individuals in society, various other cyber attacks are

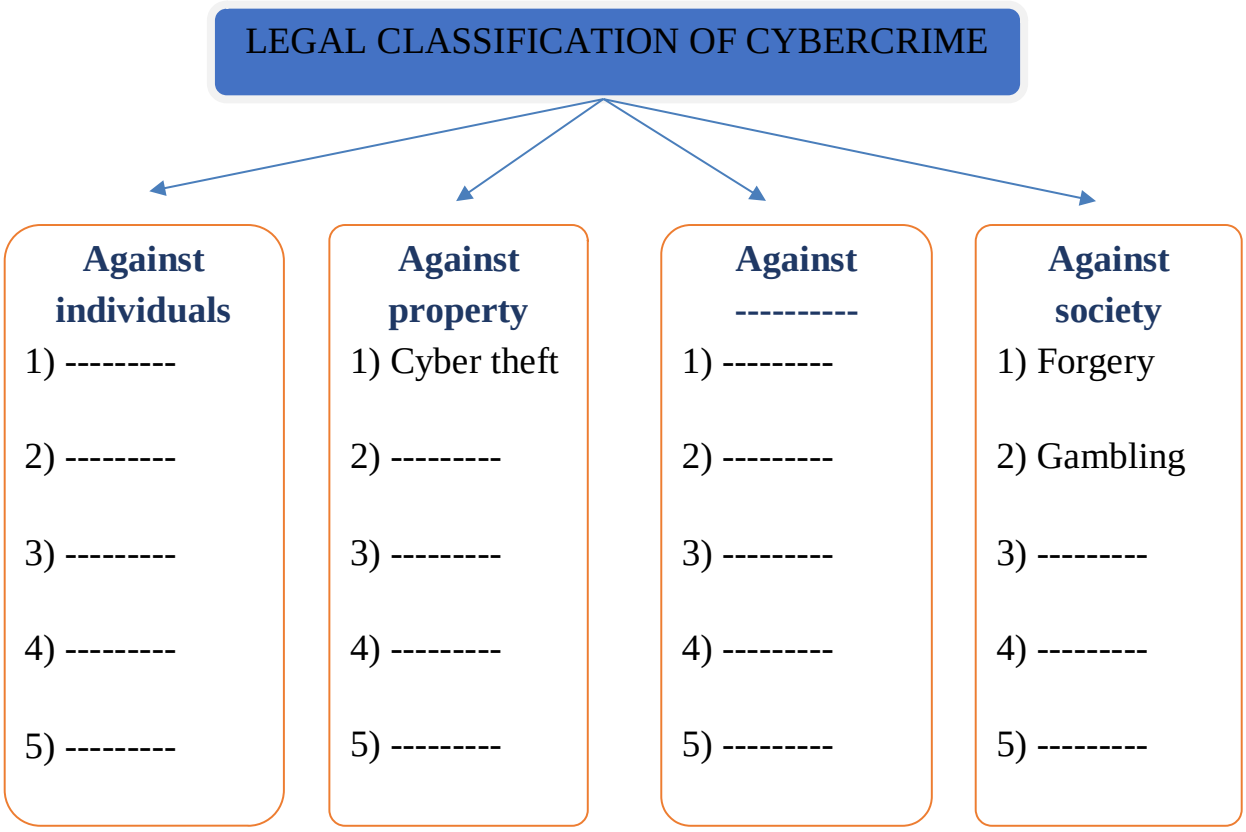
	launched against the community at large. Unfortunately, it is not difficult to cover cybercriminals' track. These unlawful acts are committed with the intention of causing harm or such alterations to the cyberspace, which will automatically affect the large number of people of society. These are finance related crimes, forgery, online gambling, sales of illegal articles, and trafficking.
4. Cybercrime against government or organizations	d. To prevent the cybercrimes, individuals and governments need to understand the crime schemes in the cyberspace and the contemporary and continuing Internet trends and behavior of the criminals. In terms of law, cybercrimes can be categorized as crimes against individuals, property, organizations and governments.
6. Cybercrimes against society	e. The second category of cybercrimes is against property. Intellectual Property Crimes, cybersquatting, cyber vandalism, transmission of malware that disrupt functions of the system or create malfunctioning of the attached devices, cyber trespassing, Internet time thefts are few of the most popular cybercrimes against property. Cyber theft of Intellectual Property (IP) is one of them. Cyber theft of IP means stealing of copyrights, trade secrets, patents etc., using internet and computers. Generally, the stolen material is sold to the rivals or others for further sale of the product. This may result in the huge loss to the company who originally created it.

Exercise 52

Find crime idioms in the text and translate sentences with them.

Exercise 53

Summarize information from the text "Legal classification of cybercrime" and complete the gaps in the picture below:



LISTENING I

Exercise 54

You are going to watch a video "What is cybercrime?" at https://www.youtube.com/watch?v=Ls8jyO46bmI

a. BEFORE YOU WATCH. Answer the questions:

1. How do you define cybercrime?
2. Have you ever faced with cybercrime?
3. Who usually becomes a victim of such kind of crime?

b. WHILE YOU WATCH. Fill in the gaps:

(1)_____ is any criminal activity that involves a computer, networked device, or network. Cyber crime is usually committed to (2)____ profit for the cyber (3)____. However, some cybercrime targets specific devices to damage or disable them, or to spread (4)____, illegal information, images, or other (5)_____ material. Crimes like

(6)_____, (7)____, money laundering, and (8)_____ are easier to carry out than ever before.

There's no one way (9)_____ a cyber attack. Cyber criminals use a variety of methods and techniques such as (10)_____, (11)_____or (12)_____attacks, (13)_____ campaigns, and (14)_____. Many cyber attacks rely on the (15)_____activating malware with clicks or downloads, or falling for fake requests for money, information, or access.

c. AFTER YOU WATCH. Answer the questions:

1. What does the cybercrime involve?
2. What is the aim of cyber criminals?
3. What types of cybercrimes are enumerated in this video?
4. What methods do the offenders use?
5. What are the consequences of cyber-attacks for businesses?

Exercise 55

Internet activity

Group work. Study information cybercrime in, the UK, the USA and the Russian Federation.

Visit the official web portal of the UK National Crime Agency: https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime

US department of state site: https://www.state.gov/cybercrime

Information security and cybercrime in Russia - statistics & facts:

https://www.statista.com/topics/7335/information-security-and-cyber-crime-in-russia/#topicOverview

b. Share the information you have learnt with your group.

SPEAKING I

Exercise 56

Pair work. Work with a partner and discuss the following:

Cybercrime can cost consumers large sums of money, and it is even more expensive for businesses, including banks and other credit card issuers. Nevertheless, when cybercriminals are caught and convicted, they are rarely ordered to pay damages or face long prison sentences. Do you believe that stiffer sentences will reduce cybercrime? Why or why not?

Exercise 57

a. Jigsaw activity. Group work. The class is divided into 2 "expert" groups (A, B). Each group reads one of the texts below. For example, Group A reads the Text "Google data case to be heard in supreme court", Group B reads the Text "Lapsus$: two UK teenagers charged with hacking for gang". Then the groups are re-mixed. Now each expert has to teach his new group his knowledge on the topic. After exchanging the information, be ready to answer the questions of your group mates.

TEXT A
GOOGLE DATA CASE TO BE HEARD IN SUPREME COURT

Mr Lloyd alleged that between 2011 and 2012 Google cookies collected data on health, race, ethnicity, sexuality and finance through Apple's Safari web browser, even when users had chosen a "do not track" privacy setting.

The case aimed to get compensation for the 4.4 million affected users.

It was the first-of-its-kind case in the UK. Although class actions - where one person brings a case on behalf of many - are common in the US, in the UK they can only be brought on an opt-in basis, meaning all those involved have to give their consent.

The Google case

Initially, the Google case was dismissed by the High Court, which ruled it was difficult to calculate how many people had been affected or whether they had suffered damage as a result of the breach.

But the Court of Appeal later ruled that the case Mr Lloyd was bringing was a suitable way for people to seek mass redress for data breaches.

Google appealed against that decision and the case has now reached the Supreme Court, where TechUK is one of several groups hoping to get it dismissed.

The group, which represents Google among others, argues that it could open the floodgates for mass litigations and seriously damage small firms who could face large penalties.

"This massively raises the liability for people providing data-driven services in the UK, which is most of the digital economy," said Antony Walker, TechUK's deputy chief executive.

Claimant Richard Lloyd said he hoped the case "could establish a form of fair redress for data misuse that doesn't currently exist in this country".

"It is about giving millions of consumers access to justice when their rights are abused by global tech giants."

Julian Copeman, partner at law firm Herbert Smith Freehills, told the BBC the case could go either way.

"There are two ways of looking at this: would allowing opt-out class actions for data claims increase access to justice, allowing companies to be held to account for what they do with their clients' data?

"Or would this simply benefit the funders and claimant law firms, while damaging business and clogging up the court system, with affected individuals only receiving nominal amounts at the end of the case?"

If the case goes ahead it could mean businesses dealing in data stand to lose a lot of money, Mr Copeman added.

"Although the amount per head that claims may win would probably only be small sums of money for each individual, given the number of claimants represented, even a small amount per head will add up to huge sums. This represents a serious problem for businesses, however large they are."

https://www.bbc.com/news/technology-56901364

TEXT B

LAPSUS$: TWO UK TEENAGERS CHARGED WITH HACKING FOR GANG

A 16- and 17-year-old appeared at Highbury Corner youth court, in London, on Friday charged with a number of cyber-offences.

The two boys have been released on bail, subject to certain conditions.

They were arrested as part of an international police investigation into the Lapsus$ gang, which has hacked major tech firms including Microsoft.

Both teenagers are charged with three counts of unauthorised access with intent to impair operation of, or hinder, access to a computer, and two counts of fraud by false representation.

The 16-year-old, has also been charged with one count of causing a computer to perform a function to secure unauthorised access to a programme.

In court, the 17-year-old wore a dark blue Adidas T-shirt and grey tracksuit bottoms. The 16-year-old wore a grey tracksuit.

Prosecutor Valerie Benjamin said the case should be sent to crown court due to its complex nature and the sums allegedly involved.

Legal restrictions related to the ages of suspects mean the names or personal details about the boys cannot be revealed.

The Lapsus$ group has successfully breached major firms such as Microsoft, and then bragged about it online.

The FBI has launched an appeal for information about the people behind the hacking crew.

Last week City of London Police which is leading the international investigation into Lapsus$, announced that it had arrested seven people between the ages of 16 and 21 in the UK.

Around the same time as news of the arrests emerged, Lapsus$ told its 45,000 followers on Telegram that some of its members were taking "a vacation".

On Wednesday, it started posting again - releasing stolen material from a software development company with headquarters in Argentina.

https://www.bbc.co.uk/news/technology-60953527

LISTENING II

Exercise 58

You are going to watch the video "What is phishing?" at https://www.youtube.com/watch?v=9TRR6lHviQc&t=27s

a. BEFORE YOU WATCH. Answer the question:

Why are identity theft related crimes on the rise?

b. WHILE YOU WATCH.

a. Answer the questions:

1. How do you spell the name of the crime referred to in the video?

2. Is it right or wrong to behave like this?

b. Watch the video for the second time and say:

1. What does phishing mean?
2. Is it dangerous to do business online?
3. What personal information do scammers want to get their hands on?
4. How can you avoid being a victim of a phishing scam?
5. What examples of a phishing scams does the speaker describe?
6. What is the best way to detect phishing emails?
7. How can you prevent identity theft and what should you do to protect your personal data?

c. AFTER YOU WATCH. Give the examples of identity theft. Have you ever been a victim of such a crime?

Exercise 59

a. Phishing and fishing are homophones: the two have the same pronunciation, but differ in spelling and meaning. Study the homophones in the box and put them in the correct sentences below:

new /knew	sauce/source	site/sight	find/fined	steal /steel
male/mail	passed/past	higher/hire	court/caught	here/hear

1. The RF Constitution - is the main (1)___ of law.
2. The most difficult part of this job is understanding the (2)____ technology.
3. Many women in IT earn less than their (3)___colleagues.
4. Inventors know that someone is always going to try to (4)___ their designs.
5. In the USA the social network was (5)____for violating the law on the protection of children's privacy on the Internet.
6. The EU has (6) ___ its first cyber security law.
7. The changes in legislation made it easier for companies to (7)____ foreign workers.
8. The Supreme (8) ___ of the United Kingdom is the highest court of appeal for civil cases in the UK, and criminal cases from England, Wales and Northern Ireland.
9. The internet (9)___ was used for illegal activities and cybercrimes.

10. During the trial, the judge decided to (10)___ witnesses and rescheduled the hearing for December 17.

b. Think of your own examples of homophones.

Exercise 60

Internet activity

a. Work in groups of three. Each student reads about one of the landmark cybercrime cases:

identity theft: https://www.aura.com/learn/identity-theft-stories-cases https://www.phonexia.com/blog/the-4-biggest-identity-theft-frauds-in-modern-history/

phishing: https://www.itgovernance.eu/blog/en/the-5-biggest-phishing-scams-of-all-time

ransomware: https://gatefy.com/blog/real-and-famous-cases-ransomware-attacks/

b. Share the information with your group. What was the crime? What happened? What was the damage? What was the sentence for the crime?

SPEAKING II

Exercise 61

Imagine that you have to make a report about different types of cybercrime. You may choose the topic for your report from the following:

1. Cybercrime as a global problem;
2. Cybercrime: the ways of stealing identity and money;
3. Legal categories of cybercrime;
4. Cybercrime in the USA, the UK and Russia;
5. Importance of digital education and raising awareness on cybercrime;
6. What is cyber fraud?
7. Who are the victims of cybercrime?

STEPS OF MAKING A REPORT

1. Define a topic of your report and the aim of your report.
2. Identify the key points.
3. Search the Internet for additional information on your topic. For example, visit the following sites:
https://cybersecurityventures.com/
https://www.kaspersky.com/resource-center/threats/what-is-cybercrime
4. Write out all the necessary terms and their definitions.
5. Structure your report:

Part	The objective	Phrases
Introduction	It provides an overview of the topic. The length of this part depends on the target reader's or listener's level of knowledge. Here you should explain the purpose of the report, provide necessary background information, and outline the plan of your presentation.	I am going to speak about… The aim of my report is… First, I'll tell you about… Second, … Third, … Finally, …
The main body	The ideas presented in the introduction are expanded. The logical development of these ideas should be consistent, relevant, and clear.	The key thing to say about … is ... The main point to make about … is ... Let's turn to / move on to ... Another interesting thing to say about … is … Finally, I'd like to say a few words about …
Conclusion	The conclusion summarizes all the information presented in the main body of the report. It should not contain any idea that has not been previously mentioned in this paper.	In conclusion, ... To sum up, ... Does anybody have any questions?

6. Get ready to ask questions.
7. While listening to the other students' reports, take notes. It will help you to remember the necessary information.

READING III

Exercise 62

a. Read and translate the interview with Evgeny Kaspersky the founder and the head of Kaspersky Lab about cybercrime in Russia.

b. Match the questions to the answers:

1. Russian hackers are almost a brand. How long will they be able to keep the leadership?
2. Who is more difficult to protect from cyber-attacks - private users or companies?
3. How much has the number of cyber-attacks increased over the past year?
4. Digital Hygiene: Is there enough attention paid to this topic in Russia?
5. Why do so many people get caught up in phone scams in spite of the widespread warning? Who should deal with this problem?
6. How to protect personal data today, when they require registration, QR-codes and so on everywhere?

CYBERCRIME IN RUSSIA

A	Unfortunately, we see an annual increase in cyber-attacks against private users. We have detected an average of 380,000 new malicious files per day this year, an increase of 5.7% over last year. We see an increase in attacks on industrial systems as well. Manufacturing companies in general are very attractive targets for cybercriminals; attacks against them provide direct financial gain and allow the attacker to expect access to valuable information. In 2022, we have noticed an interest in industrial enterprises from major cybercriminal groups.
B	I would say that if private users and companies are protecting their information systems responsibly, it is just as easy to protect them. Companies are more likely to be targeted by cybercriminals that are more serious and become victims of targeted attacks, e.g. phishing, because attacks against them bring more profit to the perpetrators.

C	Overall, online activity is still at its peak, since many people continue to work remotely and use more and more digital devices. It is very important that users improve their digital literacy and update their security solutions on time. Awareness of cyber threats is much higher now than, for example, ten or even five years ago. Nevertheless, this literacy is an ongoing effort that needs to be taught from the high school level.
D	It seems to me that this problem is as old as the world. Unfortunately, scammers were, are and will be. They are always looking for a weak link that can easily be cheated. Now they probably just have more opportunities. We have an application called “Kaspersky Who Calls” to combat telephone scammers. It also cuts out all kinds of mobile audio spam. Of course, you have to be vigilant and follow the basic rules of keeping your personal data and financial data safe.
E	Unfortunately, no one is safe from data leaks. Therefore, it is almost impossible to protect your data completely. Nevertheless, this is a question of digital hygiene. You should not register at suspicious sites or leave your personal data without extreme necessity. Do not use the same easy password everywhere. In fact, passwords should be changed as often as possible, and you have to use two-factor authentication everywhere you can.
F	The leadership of Russian hackers is the reverse side of the fact that Russia still has an educational system that trains excellent developers. Russian programmers are the best in the world. Once I was asked in Switzerland: "Are you thinking of relocating development from Russia to Europe?" I replied: "If I ran a Swiss company, I would think about relocating development to Russia.” As long as we train the world's best programmers, we will also have the world's best hackers.

c. Answer the question: How did 2022 change the sphere of cybercrime and what is going to happen in 2023?

WRITING

Exercise 63

a. Do you know how to write a summary?

You can find some rules of summary writing at: https://www.youtube.com/watch?v=QJdYjNCKCj4&t=473s

b. Study the useful phrases for a summary:

I'll make a summary of the text. The title of the text is…
The text deals with / covers / describes…
At the beginning of the text the author writes that…
The text says (mentions, underlines, stresses) that…
The text goes on to say…
It is interesting to note…
In addition….
At the end of the text…
In conclusion the author writes…

c. Read the text about the famous cybercrime and write a summary using the phrases from b.

A BYTE OUT OF HISTORY
$10 MILLION HACK, 1994-STYLE

It was hardly the opening salvo in a new era of virtual crime, but it was certainly a shot across the bow.

Two decades ago, a group of enterprising criminals on multiple continents—led by a young computer programmer in St. Petersburg, Russia—hacked into the electronic systems of a major U.S. bank and secretly started stealing money. No mask, no note, no gun—this was bank robbery for the technological age.

Our case began in July 1994, when several corporate bank customers discovered that a total of $400,000 was missing from their accounts. Once bank officials realized the problem, they immediately contacted the FBI. Hackers had apparently targeted the institution's cash management computer system—which allowed corporate clients to move funds from their own accounts into other banks around the world. The criminals gained access by exploiting the telecommunications network and compromising valid user IDs and passwords.

Working with the bank, we began monitoring the accounts for more illegal transfers. We eventually identified approximately 40 illegal transactions from late June through October, mostly going to overseas bank accounts and ultimately adding up to more than $10 million. Meanwhile, the bank was able to get the overseas accounts frozen so no additional money could be withdrawn.

The only location where money was actually transferred within the U.S. was San Francisco. Investigators pinpointed the bank accounts there and identified the owners

as a Russian couple who had previously lived in the country. When the wife flew into San Francisco and attempted to withdraw funds from one of the accounts, the FBI arrested her and, soon after, her husband. Both cooperated in the investigation, telling us that the hacking operation was based inside a St. Petersburg computer firm and that they were working for a Russian named Vladimir Levin. (See the sidebar for more on the San Francisco angle of the case from one of the agents who worked it.)

We teamed up with Russian authorities—who provided outstanding cooperation just days after a new FBI legal attaché office had been opened in Moscow—to gather evidence against Levin, including proof that he was accessing the bank's computer from his own laptop. We also worked with other law enforcement partners to arrest two co-conspirators attempting to withdraw cash from overseas accounts; both were Russian nationals who had been recruited as couriers and paid to take the stolen funds that had been transferred to their personal accounts.

In March 1995, Levin was lured to London, where he was arrested and later extradited back to the United States. He pled guilty in January 1998.

Believed to be the first online bank robbery, the virtual theft and ensuing investigation were a needed wakeup call for the financial industry and for law enforcement. The victim bank put corrective measures in place to shore up its network security. Though the hack didn't involve the Internet, the case did generate media coverage that got the attention of web security experts. The FBI, for its part, began expanding its cybercrime capabilities and global footprint, steadily building an arsenal of tools and techniques that help us lead the national effort to investigative high-tech crimes today.

https://www.fbi.gov/news/stories/a-byte-out-of-history-10-million-hack

d. Write a summary of the text you have read.

TRANSLATION PRACTICE

Exercise 64

Translate the text into Russian.

CYBER THEFT

In cyberspace, thieves are not subject to the physical limitations of the "real" world. A thief can steal data stored in a networked computer with network access from anywhere on the globe. Only the speed of the connection and the thief's computer equipment limit the quantity of data that can be stolen.

Not surprisingly, there has been an increase in identity theft, which occurs when the wrongdoer steals a form of identification—such as a name, date of birth, or Social Security number—and uses the information to access the victim's financial resources. This crime existed to a certain extent before widespread use of the Internet. For instance, thieves would "steal" calling-card numbers by watching people using public telephones, or they would rifle through garbage to find bank account or credit-card numbers. The identity thief would then use the calling-card or credit-card number or withdraw funds from the victim's account until the theft was discovered. The Internet has provided even easier access to private data. Frequent Web surfers surrender a wealth of information about themselves without knowing it. Many Web sites use "cookies" to collect data on those who visit their sites. The data can include the areas of the site the user visits and the links on which the user clicks. Furthermore, Web browsers often store information such as the consumer's name and e-mail address. Finally, every time a purchase is made online, the item is linked to the purchaser's name, allowing Web retailers to amass a database of who is buying what. Identity theft criminals have devised even more ingenious methods.

As many consumers are discovering, any information that can be collected can be stolen. About 3 percent of all American households—3.6 million in total—report that at least one member has been the victim of a recent identity theft. In reality, the cyber criminals who steal people's identities normally do not use them. Instead, they sell the information on the Internet. Several hundred Web sites sell black market private data, most of them hosted on Russian servers and out of reach of U.S. authorities. Among identity thieves, stolen credit-card numbers are sold for as little as $1 each, while a complete identity, including date of birth, bank account, and government-issued identification numbers, can be purchased for less than $15. Many online criminals are turning to synthetic identity theft. Rather than pilfering a "true" identity, they use a fabricated identity to gain access to online funds.

Roger LeRoy Miller Business Law Today, South-Western, Cengage Learning© 2014 pp.175-176

TEST 2.
BASICS OF CYBERCRIME

Choose the correct word(s) to complete the sentences:

1. The men were put on trial under the UAE's cybercrime law, which _____ in 2012.
a) implemented;
b) implement;
c) was implemented;
d) is implemented.

2. You need to deal _____ organized fraud.
a) on;
b) with;
c) in;
d) out.

3. If that SIM-card or phone is then used to _____ a crime, the person involved can be tracked.
a) cut;
b) commit;
c) combat;
d) convict.

4. _____ is the crime committed via a computer with the intent to corrupt another individual’s personal and financial information stored online.
a) Harassment;
b) Gambling;
c) Spamming;
d) Cyber fraud.

5. The most common form of _____ is when someone uses another person's information for financial gain.
a) identity theft;
b) harassment;
c) espionage;

d) gambling.

6. _____is the activity of betting money, for example in a game.

a) Spamming;
b) Phishing;
c) Gambling;
d) Identity theft.

7. Cybercrimes against _____ include violation of privacy, harassment of a person through e-mail spoofing, hacking, cyber stalking, defamation, cheating, fraud, credit card frauds, gambling etc.

a) property;
b) persons;
c) organizations;
d) society.

8. Intellectual Property Crimes, cybersquatting, cyber vandalism, cyber trespassing, Internet time thefts are cybercrimes against _____.

a) persons;
b) organizations;
c) property;
d) society.

9. Cybercrime against _____mainly includes unauthorized access of computer, password sniffing, denial of service attacks, malware attacks, industrial espionage, forgery, web-jacking etc.

a) organizations;
b) persons;
c) property;
d) society.

10. What would you do if the offenders _____ the money from your card?

a) stole;
b) steal;
c) have stolen;
d) will steal.

11. The evidence *may not* be useful if it _____ illegally.

a) obtained;
b) is obtained;
c) obtain;
d) will be obtained.

12. What mechanisms _____ if you want to protect copyright online?
a) you applied;
b) you apply;
c) would you apply;
d) will you apply.

13. If you _____ e-mail for work or communication, then you _____ what spam is.
a) used, know;
b) use, knew;
c) use, know;
d) will use, will know.

14. If you had been more attentive, you _____ a victim of cyber fraud.
a) would not have become;
b) would not become;
c) will not become;
d) had not become.

15. Even if hackers and cybercriminals _____ to gain access to said information, it would be of no use to them.
a) are;
b) were;
c) had been;
d) have been.

Unit 3.
The Computer's Role in Crime

LEAD-IN

Work in pairs and explain how you understand this quotation:

"One single vulnerability is all an attacker needs"

by Window Snyder, an American computer security expert

How would you complete the saying?

"If you spend more on coffee than on IT security, you will be hacked. What's more, you deserve to be hacked"

by Richard Clarke, an American national security expert

KEY TERMS

antivirus software	антивирусное ПО
bug bounty (inf)	1) выявление ошибок и уязвимостей в компьютерной программе или системе (за вознаграждение) 2) вознаграждение за выявление ошибок и уязвимостей в компьютерной программе
chief security officer (CSO)	начальник службы безопасности
classified	не подлежащий оглашению
compromise (v)	нарушить секретность, скомпрометировать
computer crime	преступления, связанные с использованием компьютеров
computer trespass	вторжение в частное электронное пространство
computer virus	компьютерный вирус
computer worm	компьютерный червь

con (inf)	1) (n) афера 2) (v) обманывать
counterfeiting	изготовление контрафактной продукции
digital (computer) forensics	цифровая (компьютерная) криминалистика
infiltrate	тайно проникнуть
logic (software) bomb	логическая бомба
mishandling	небрежное, ненадлежащее обращение
misuse	злоупотребление, нецелевое употребление
scam (inf)	1) (n) обман 2) (v) обманывать
software piracy	нарушение авторских прав на программное обеспечение
social engineering	метод проникновения в защищенные системы, основанный на использовании социальной психологии
Trojan horse	троянский конь (вредоносная программа)
unlawful access	неправомерный доступ
vulnerability	уязвимость

VOCABULARY

Exercise 65

a. What parts of speech are the following words:

compromised, cyberfraud, mishandling, unlawful, perpetration, negligence, liability, liable, neglect, extortion, extort, scammer, vulnerability, vulnerable, classification.

b. Identify suffixes, prefixes and translate the words.

Exercise 66

Which word is odd? Why?

mitigate	lessen	worsen	soften
computer crime	murder	phishing	spamming

infiltrate	sneak into	break into	slink into
extort	ransom	blackmail	donate
perpetration	inaction	commission	committing
software	application	hardware	program
mishandle	mess up	control	make a mistake
irresponsibility	liability	guilt	blame

Exercise 67

a. Match the words with similar meaning.

1) mitigate	a) malicious code
2) compromise	b) threat
3) liability	c) minimize
4) counterfeit	d) abuse
5) virus	e) jeopordise
6) perpetration	f) responsibility
7) misuse	g) commission
8) vulnerability	h) bootleg

b. Match the words with opposite meaning.

1) perpetration	a) precaution
2) piracy	b) secure
3) antivirus software	c) authorized
4) digital forensic researcher	d) inaction
5) vulnerable	e) open source information (OSI)
6) classified	f) malware
7) negligence	g) scam artist
8) unlawful	h) copyright

Exercise 68

Match the words to the definitions.

1) computer trespass	a) a program that seems useful but is designed to be harmful, for example by destroying information
2) bug bounty	b) a piece of code intentionally inserted into a software system that

	will set off a malicious function when specified conditions are met
3) copyright	c) the crime of secretly taking money that is in your care or that belongs to an organization or business you work for
4) CSO	d) the practice of manipulating people in a way that they give away confidential information online
5) embezzlement	e) a C-suite executive responsible for a company's physical and digital security
6) Trojan horse	f) the act of crossing invisible, yet established, boundaries of ownership in an online environment
7) computer worm	g) the legal right to control the production and selling of a book, play, film, photograph, or piece of music
8) computer virus	h) a self-sufficient program that is designed to damage computer systems by making copies of itself and preventing the computer from working correctly
9) software piracy	i) a reward offered to a person who identifies an error or vulnerability in a computer program or system
10) logic (software) bomb	j) a malicious executable code attached to another executable file that can be harmless or can modify or delete data
11) social engineering	k) the practice of downloading and distributing copyrighted software digitally without permission

Exercise 69

a. Match the word combinations and then translate them.

1) copyright	a) counterfeiting

2) gross	b) artist
3) software	c) violation
4) antivirus	d) documents
5) bug bounty	e) measures
6) compromised	f) fraud
7) cybersecurity	g) password
8) scam	h) negligence
9) social engineering	i) hunter
10) classified	j) software

b. Complete the following sentences using the words and word combinations from the previous tasks.

1. Cybercriminals who use _____ attacks look for weaknesses in human nature.
2. This makes your Extranet account a tempting target for cyber criminals and _____, who will try many different things to gain access to the data held in your account.
3. Microsoft gave _____ starting points to look for bugs by pointing out features that are unique to its new browser.
4. "There are attacks attempting to shut down our servers," said Ken Silva, VeriSign's _____.
5. Comey also said that it would have been inappropriate to charge Clinton, seeking to become the first U.S. female president, under a 1917 U.S. law making "_____" a crime.
6. The best defense against a _____ is to never run a program that is sent to you.
7. Hidden within the kernel is a _____, malicious code designed to execute under circumstances I've programmed.
8. Make sure that any computer you use to access social media has _____.
9. Activation is aimed at reducing _____, thereby helping to ensure that Microsoft customers receive the software quality that they expect.
10. Clinton said she never sent or received emails that were marked as _____.

Exercise 70

Match the parts of the sentences:

1. Not only do the devices themselves pose risk as an entry point or Trojan Horse for malware, the infected devices can used to perpetrate	a) trespass, grand larceny of fourth degree.
2. The police are concerned at the growing trend of cybercrime and the misuse	b) social networks and perhaps even influence public opinion.
3. Some are sophisticated enough to infiltrate	c) password for other services up to a year after the leak.
4.Ask to have these issues fixed before you sign	d) complex phishing scams intended to unlock company information.
5. The Company has, and will continue to develop any tools necessary to identify fraudulent and/ or unlawful	e) to malicious attacks and even fraud.
6. As a result, Mr. Drake faced 10 felony charges involving mishandling	f) the lease and do not sign until these issues are dealt with.
7. Lack of synchronization can serious problems and can even leave a system vulnerable	g) mishandling of classified data while secretary of state through the use of an unsecured, home-brewed bathroom server
8. Mr. Alderson, I declare you guilty of computer hacking, computer	h) of information and telecommunications technologies in multiple forms of crime.
9. Trump's comment came against the backdrop of Hillary Clinton's gross	i) of classified information and obstruction of justice, which a judge wisely dismissed.
10. Over 70% of users employed a compromised	j) access and use of our Online Trading Facility.

Exercise 71

Translate these sentences from Russian into English using the words and word combinations from the previous tasks.

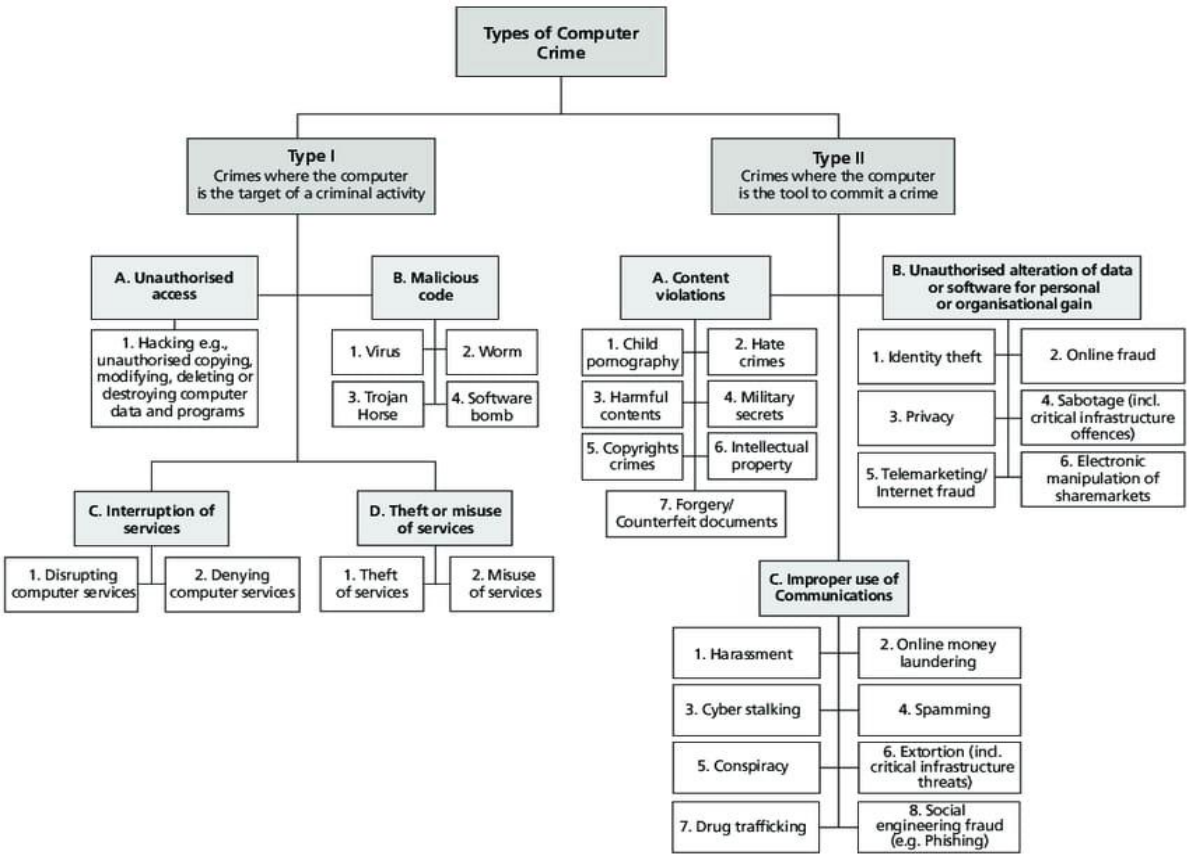
1. Кроме того, количество схем цифрового вымогательства выросло на 200% со второй половины 2020 года.
2. Третья проблема – это пиратство и нарушение авторских прав.

3. Уязвимость была исправлена, и исследователи получили значительную сумму в качестве вознаграждения за выявление ошибок.
4. Облачная криминалистика – это разновидность цифровой криминалистики, основанная на уникальном подходе работы с облачными средами.
5. Рассмотрим типичные категории компьютерных преступлений и те, негативные последствия, с которыми из-за них сталкивается общество.
6. Большая часть утечек данных является результатом грубой халатности со стороны работников той или иной компании.
7. Двухуровневая авторизация помогает защитить учетную запись от несанкционированного доступа от фишинговых атак и других киберпреступлений в случае, если вы скомпрометировали свой пароль.
8. Вы можете использовать логическую бомбу, чтобы проникнуть на сервер.
9. Для этого ему пришлось разработать математическую модель компьютерного вируса.
10. Большая доля пользователей не использует регулярно обновляемое антивирусное ПО.

READING I

Exercise 72

a. BEFORE YOU READ. Look at picture below depicting types of computer crimes according to the role of computer in them. Examine the table.



b. Read the supplementary classification of cyber crimes. Express your own opinion. Is it more exhaustive?

THE COMPUTER'S ROLE IN CRIME

As a knife might be both an assassination weapon and a weapon of self-defense and it might be stolen, counterfeited and lost, it would be naive and unreasonable to think that a computer couldn't be used in different ways. Lawyers classify computer crimes from the perspective of the role computer plays in crime.

The U.S. Department of Justice broadly defines **computer crime** as "*any violation of criminal law that involves knowledge of computer technology for [its] perpetration, investigation, or prosecution".* Here, we should look at the classifications given by American researches.

The first classification distinguishes three categories of computer, or cyber, crimes:

1. The computer is the *object* of a crime, such as when the computer itself or its software is stolen.

2. The computer is the *subject* of a crime, just as a house is the subject of a burglary. This type of computer crime occurs, for example, when someone “breaks into” a computer to steal personal information such as a credit-card number.

3. The computer is the *instrument* of a crime, as when someone uses a computer to con a gullible person out of a great deal of funds.

It is important to bear in mind that a number of the white-collar crimes (i.e., crimes that typically occur only in the business context), such as fraud, embezzlement, and the theft of intellectual property, are now committed with the aid of computers and are thus considered computer crimes. However, the term "cyber crime" is more suitable if one wants to describe any criminal activity occurring via a computer in the virtual community of the Internet.

Business Law Today. Text & Summaraized Cases / Roger LeRoy Miller, Gaylord A. Jentz, Herbert D. Kelleher. pp. 172-173.

Exercise 73

Look at brief descriptions of cases below. Use the classifications from the picture and the text and try to categorize the crimes described.

1. God Guluva shared that his laptop got stolen and then he received an email from his own account. The thief wrote to Guluva that he stole the laptop the previous day, as he needed money to survive. The thief realised that Guluva was busy with a research proposal and attached the relevant files stored in the laptop to the email. The thief also asked Guluva to tell if he needed any other files before 12 pm Monday as a potential buyer was waiting for the stolen laptop.

2. The user CVI games reported on the Apple web-site for developers that his application was stolen, republished and used to earn money. The developer said, "The thing that bugs me a lot is that the clone of my app is ranking really high! That is MY work and they are obtaining money and visibility with it". Also, he blamed the thieves for republishing stolen apps on routine basis.

3. A man has been accused of allegedly fleeing with 17 200 Rs from an ATM in Ghaziabad on May 6. Using an infected USB drive, the malware was transferred and the system rebooted. The malware used on an ATM generates a code, which the crooks send to their gang members, who then convert the code to a password. Next, as soon as the password is applied, the ATM starts dispensing cash.

4. In August 2019, Fstoppers reported a phishing campaign launched on Instagram. One victim received a private message from what appeared to an official

North Face account alleging a copyright violation, and prompted him to follow a link to a seemingly legitimate website where users are asked to input their login credentials. Victims who fell for the trap ultimately provided hackers with access to their account information and other personal data linked to their Instagram account.

5. West Virginia-based Coplin Health Systems is notifying 43,000 patients of a potential data breach due to the theft of a laptop from an employee's car. Officials discovered the theft on Nov. 2. And while the organization equipped the laptop with security tools and was password-protected, it failed to encrypt data stored on the hard drive. Data on the laptop included patient names, Social Security numbers, financial information, addresses, dates of birth and medical data.

LISTENING I

Exercise 74

Watch the video of Fred Abignale talking cyberscamming and sybersecurity at https://www.youtube.com/watch?v=FsXlThlI7Ic

a. BEFORE YOU WATCH. Look at the questions below and try to answer them. Then watch the video and check your guesses.

1. Who is a CSO (Chief Security Officer)? What does he or she do?
2. What basement information is needed to steal one's identity?
3. Which form of payment is more reliable and secure? Credit card or debit card?
4. Is it good to be sceptical in order not to be scammed?

b. WHILE YOU WATCH. Look at the sentences below and fill in the gaps.

1. And in that book I looked at every single _____ that perpetrated from the most amateur to the most sophisticated.
2. Crime has changed a lot. 40 years ago, it was all about _____, _____, financial crimes.
3. They were very _____, for the hacker got in, sat there for several months to decide what to steal, then stole 148 million identities, 12 million driver's licenses.
4. I always remind people that if you tell me on Facebook where you were born and your _____ that's 98% of me stealing your identity.
5. If you have to go buy a car, you _____ it [credit] to the dealer so they can run the credit to sell you the car, but other than that nobody can see it.

6. I would do everything in my best to protect my number, but if someone gets it and charges a million dollars on my credit card tomorrow, under federal law I have zero _____.
7. They say, "Son you have no credit, you don't even have a credit file with the credit bureau, so your parents will have to co-sign _____".
8. Whose responsibility do you believe _____ are? Is it the responsibility of big institutions or is it the responsibility of the potential victims?
9. If I've _____ my information to a bank, or credit bureau, or retailer, I'm entrusting them to keep my information safe.
10. But if the fines were a big percentage of their company's value I think you'd see a lot less of the negligence _____ companies.
11. I just dealt with a woman in Iowa that lost she's 92 lost $400,000 of her life savings to a _____ game in Jamaica.
12. They're fighting a very difficult fight, they're dealing with criminals all over the world, not just _____, but they're also dealing fighting with their own company.

c. AFTER YOU WATCH. Group work. Discuss the content of the video. Answer the questions:

1. Which tip by Frank was the most interesting and effective? Why?
2. Is he right about companies' liabilities for keeping customers' data secure? Why?

Exercise 75

Read another interview about cybersecurity given by Frank Abignale to the *WIRED* web-site. Unfortunately, the questions and the responses are mixed. Read the responses and match them to the appropriate questions.

Questions	**Responses**
1. How would the technology available today have affected your ability to con people in your early years?	d. No. They are breaking the law. But I do understand that some of them are extremely creative. A lot of what happens is our fault. For example, I've been involved with the FBI for 37 years. Every case involving cybercrime that I've been involved in, I've never found a master criminal sitting somewhere in Russia or Hong Kong or Beijing. It always ends up that somebody at the company did something they weren't supposed to do. They read an email, went to

a website they weren't supposed to. So they opened the door that allowed the person to get in. It's not that these people are that talented but they wait knowing that with a company of 10,000 employees someone is bound to open the door. They just wait for that door to be open.

2. Do new technologies make it easier to find all the information you need?

e. The biggest thing that concerns me is when we start getting countries using cybercrime to shut down infrastructure, electricity, communications systems, the internet etcetera. But crime goes to wherever there's money to be made.

Last year the Inland Revenue Service (IRS) paid out more than $5 billion in false tax returns. People use online tax services like TurboTax and file for taxes under someone else's name and then they get the refund due to the person before they know about it. By the time they file their own tax return, they've already paid out money and the victim has to wait around a year to get things straightened out.

3. Can you give me some examples of how technology breeds crime?

g. It's an education thing. I speak at a lot of universities and people are always worried about Facebook and when I explain how to use it properly they immediately go back and make those changes.

Imagine if you are 14-year-old kid and you just read a book about the Nazis. So you get on Facebook and say, "wow, I think the Nazis are cool" or "I love the Nazis". Then six years later you apply to university or a job and they go to your Facebook page and see that statement and they don't hire you. Be very careful of what you say on your Facebook page.

4. Do you have any respect for cyber criminals?

b. Fifty years ago, information was hard to come by. When you created a cheque you had no way of knowing where in reality British Airways' bank was, who was authorised to sign their cheques and you didn't know their account number. Today you can call any corporation in the world and tell them you are getting ready to wire them money and they will tell you the bank, the wiring number, the account number. You can then ask for a copy of the annual report and on page

three are the signatures of the chairman of the board, the CEO and the treasurer. It's all on white glossy paper with black ink – scanner ready art. You then just print it onto the cheque.

5. Which sort of cybercrime do you see as most worrying?

f. The problem you have today is that crime has become truly overwhelming and in the US white collar crime was over $950bn. It was almost a trillion dollars. So you have everything from Wall Street fraud to embezzlements to cybercrime and then you have to deal with terrorism as well. So a lot of crime is going on but there are very few resources to deal with it. This means that you have to privatise, so if you are a credit card company you are after the guys stealing $5-10 million from you. Criminals know that if they stay under certain thresholds, nobody is going to come after them. The fact that cybercrime is global makes it particularly hard. If I know someone in Russia is getting information and breaking into a bank's computer system, trying to get the Russian police to go after that person is almost impossible.

6. How well are governments coping with fighting cybercrimes?

c. If I'm in the airport in London and I take out my iPhone and take a picture of you walking through the airport, I can use PittPatt – an application that used to be used by the FBI but has been bought by Google – for facial recognition. If you are on Facebook [or you are identified by your image online somewhere else, for example a company website] I can find out who you are within seconds. If you happen to tell me where you were born, your date of birth and that kind of information then I'm 98 percent of the way to stealing your identity.

Another example is a scam involving apps that allow you to scan and deposit cheques using an iPhone. A few weeks ago we had a man out in Kansas City who sold his home and was paid with a cheque for $583,000 (£386,000). He asked for a glass of water and then scanned the cheque with his phone to deposit it into his bank account. When the lady came back, he told her that

	he'd changed his mind and would prefer for her to wire him the money. He then handed the cheque back and so the buyers then wired him another $583,000.
7. How can individuals protect themselves?	a. What I did was almost 50 years ago and it's about 4,000 times easier today to con people than when I did it. To forge a cheque 50 years ago, you needed a Heidelberg printed press, you had to be a skilled printer, know how to do colour separations, negatives, type-setting... those presses were 90 feet long and 18 feet high. There was a lot of work involved in creating a cheque.Today, you open a laptop. If you are going to forge a British Airways cheque, you go to their website, capture the corporate logo and put it in the top right corner. You then put a jet taking off in the background and make a really fancy four-colour cheque in 15 minutes on your computer. You then go down to an office supply store, buy security cheque paper and put it in your colour printer.

https://www.wired.co.uk/

READING II

Exercise 76

Read an additional to those which are above classification of cyber crimes given by Dr. David L. Carter, Ph.D., a professor in the School of Criminal Justice, Michigan State University. Discuss it with your groupmates.

DR. CARTER'S CLASSIFICATION

Another classification is given by Dr. Carter in the article called *'Computer Crime Categories. How Techno-criminals Operate'*. This classification may look more confusing and complicated but it is also more extensive. He distinguished four types of cyber crimes:

1. Computer As the Target

In such crimes, the offender uses the computer to obtain information or to damage operating programs. The offender commits the crime either by "superzapping" or by becoming a "super user". These labels mean that the offender accesses the operating

program by masquerading as the system's manager, thus giving the intruder access to virtually every file in the system.

Crimes in which the computer is the target include such offenses as theft of intellectual property, theft of marketing information (e.g., customer lists, pricing data, or marketing plans), or blackmail based on information gained from computerized files (e.g., medical information, personal history, or sexual preference). These crimes also could entail sabotage of intellectual property, marketing, pricing, or personnel data or sabotage of operating systems and programs with the intent to impede a business or create chaos in a business' operations. Unlawful access to criminal justice and other government records is another crime that targets the computer directly. This crime covers changing a criminal history; modifying want and warrant information; creating a driver's license, passport, or another document for identification purposes; changing tax records; or gaining access to intelligence files. Techno-vandalism and techno-trespass should be included in this category.

2. Computer As the Instrumentality of the Crime

In common law, instrumentality refers to the diversion of a lawfully possessed item, that is, an instrument, to facilitate committing a crime. In this category, and it is very important to note, the processes of the computer, not the contents of computer files, facilitate the crime.

Essentially, the criminal introduces a new code (programming instructions) to manipulate the computer's analytical processes, thereby facilitating the crime. Another

method involves converting legitimate computer processes for illegitimate purposes. Crimes in this category include fraudulent use of automated teller machine (ATM) cards and accounts; theft of money from accrual, conversion, or transfer accounts; credit card fraud; fraud from computer transactions (stock transfers, sales, or billings); and telecommunications fraud.

3. Computer Is All Incidental to Other Crimes

In this category of computer crime, the computer is not essential for the crime to occur, but it is related to the criminal act. This means that the crime could occur without the technology; however, computerization helps the crime to occur faster, permits processing of greater amounts of information, and makes the crime more difficult to identify or trace. Such crimes include money laundering and unlawful banking transactions, organized crime records or books, and book making. In one case, a suspect committed murder by changing a patient's medication information and dosage in a hospital computer.

4. Crimes Associated With the Prevalence of Computers

The simple presence of computers, and notably the widespread growth of microcomputers, generates new versions of fairly traditional crimes. In these cases, technological growth essentially creates new crime targets. Software piracy/counterfeiting, copyright violation of computer programs, counterfeit equipment, black market computer equipment and programs, and theft of technological equipment fall into this category.

One offense in this category occurs with relative frequency – the violation of copyright restrictions of commercial software. Initially, this offense may not seem like a serious crime; yet, the potential loss to businesses can be quite staggering.

David L. Carter, Ph.D. Computer Crime Categories. How Techno-criminals Operate. FBI Law Enforcement Bulletin. July 1995, Vol. 64, Number 7. pp 22-23.

Exercise 77

Read Dr. Carter's classification again and answer the following questions.

1. Can you tell the difference between Type 1 and Type 4 crimes? What is the distinguishing feature?
2. Is a computer necessary for committing Type 3 crimes?
3. How does the intruder get the access to files in a target system?
4. What are the two methods described of committing Type 2 crimes?
5. How can any illegal manipulation of software be classified?

Exercise 78

Examine each classification of computer crimes presented in this Chapter once again. Which one is more suitable for legal practices? Which one is more exhaustive and thorough? Give your own opinion and prove your point.

Exercise 79

Read the extract from FBI Director's statement. Paragraphs are mixed. Put them into correct order and translate the text.

STATEMENT BY FBI DIRECTOR JAMES B. COMEY ON THE INVESTIGATION OF SECRETARY HILLARY CLINTON'S USE OF A PERSONAL E-MAIL SYSTEM

So that's what we found. Finally, with respect to our recommendation to the Department of Justice:

1. As a result, although the Department of Justice makes final decisions on matters like this, we are expressing to Justice our view that no charges are appropriate in this case.

2. In our system, the prosecutors make the decisions about whether charges are appropriate based on evidence the FBI has helped collect. Although we don't normally make public our recommendations to the prosecutors, we frequently make recommendations and engage in productive conversations with prosecutors about what resolution may be appropriate, given the evidence. In this case, given the importance of the matter, I think unusual transparency is in order.

3. I know there were many opinions expressed by people who were not part of the investigation—including people in government—but none of that mattered to us. Opinions are irrelevant, and they were all uninformed by insight into our investigation, because we did the investigation the right way. Only facts matter, and the FBI found them here in an entirely apolitical and professional way. I couldn't be prouder to be part of this organization.

4. Although there is evidence of potential violations of the statutes regarding the handling of classified information, our judgment is that no reasonable prosecutor would bring such a case. Prosecutors necessarily weigh a number of factors before bringing charges. There are obvious considerations, like the strength of the evidence, especially regarding intent. Responsible decisions also consider the context of a person's actions, and how similar situations have been handled in the past.

5. To be clear, this is not to suggest that in similar circumstances, a person who engaged in this activity would face no consequences. To the contrary, those individuals are often subject to security or administrative sanctions. But that is not what we are deciding now.

6. I know there will be intense public debate in the wake of this recommendation, as there was throughout this investigation. What I can assure the American people is that this investigation was done competently, honestly, and independently. No outside influence of any kind was brought to bear.

7. In looking back at our investigations into mishandling or removal of classified information, we cannot find a case that would support bringing criminal charges on

these facts. All the cases prosecuted involved some combination of: clearly intentional and willful mishandling of classified information; or vast quantities of materials exposed in such a way as to support an inference of intentional misconduct; or indications of disloyalty to the United States; or efforts to obstruct justice. We do not see those things here.

Exercise 80

a. Read (or watch at https://time.com/4393372/james-comey-fbi-hillary-clinton-email-speech-transcript/) the whole statement and get acquainted with additional material on the Net if necessary.

b. Express your opinion on the case and discuss it with your groupmates. How would classify Hillary Clintin's deed? Answer the questions:

1. Have you known anything about the case before?
2. Do you think that James Comey's recommendations are proper and just?
3. What do you think about using corporate or state equipment for personal purposes? Should it be punishable?
4. What do you think of such a mishandling of classified information? What punishment should be for state or corporate people who act in a such grossly negligent way?

SPEAKING I

Exercise 81

Jigsaw activity

a. Group work. The class is divided into 2 "expert" groups (A, B). Each group reads one of the texts below. Group A reads Text A "Hackers Breached Colonial Pipeline Using Compromised Password", Group B reads Text B "Marriott discloses massive data breach affecting up to 500 million guests".

TEXT A
HACKERS BREACHED COLONIAL PIPELINE USING COMPROMISED PASSWORD

The hack that took down the largest fuel pipeline in the U.S. and led to shortages across the East Coast was the result of a single compromised password, according to a cybersecurity consultant who responded to the attack.

Hackers gained entry into the networks of Colonial Pipeline Co. on April 29 through a virtual private network account, which allowed employees to remotely access the company's computer network, said Charles Carmakal, senior vice president at cybersecurity firm Mandiant, part of FireEye Inc., in an interview. The account was no longer in use at the time of the attack but could still be used to access Colonial's network, he said.

The account's password has since been discovered inside a batch of leaked passwords on the dark web. That means a Colonial employee may have used the same password on another account that was previously hacked, he said. However, Carmakal said he isn't certain that's how hackers obtained the password, and he said investigators may never know for certain how the credential was obtained.

The VPN account, which has since been deactivated, didn't use multifactor authentication, a basic cybersecurity tool, allowing the hackers to breach Colonial's network using just a compromised username and password. It's not known how the hackers obtained the correct username or if they were able to determine it on their own.

"We did a pretty exhaustive search of the environment to try and determine how they actually got those credentials," Carmakal said. "We don't see any evidence of phishing for the employee whose credentials were used. We have not seen any other evidence of attacker activity before April 29."

Ransom Note

A little more than one week later, on May 7, an employee in Colonial's control room saw a ransom note demanding cryptocurrency appear on a computer just before 5 a.m. The employee notified an operations supervisor who immediately began to start the process of shutting down the pipeline, Colonial Chief Executive Officer Joseph Blount said in an interview. By 6:10 a.m., the entire pipeline had been shut down, Blount said.

It was the first time Colonial had shut down the entirety of its gasoline pipeline system in its 57-year history, Blount said. "We had no choice at that point," he said. "It was absolutely the right thing to do. At that time, we had no idea who was attacking us or what their motives were."

It didn't take long for news of Colonial's shutdown to spread. The company's system transports roughly 2.5 million barrels of fuel daily from the Gulf Coast to the Eastern Seaboard. The outage led to long lines at gas stations, many of which ran out, and higher fuel prices. Colonial began resuming service on May 12.

Soon after the attack, Colonial embarked on an exhaustive examination of the pipeline, tracking 29,000 miles on the ground and through the air to look for visible damage. The company ultimately determined the pipeline wasn't damaged.

Sweeping Network

In the meantime, Mandiant was sweeping the network to understand how far hackers had probed while installing new detection tools that would alert Colonial of any follow-on attacks – which aren't uncommon after a substantial breach, Carmakal said. Investigators haven't found any evidence the same group of hackers tried to regain access.

"The last thing we wanted was for a threat actor to have active access to a network where there is any possible risk to a pipeline. That was the biggest focus until it was turned back on," Carmakal said.

Mandiant also traced the hackers' movements in the network to determine how close they got to compromising systems adjacent to Colonial's operational technology network – the system of computers that control the actual flow of gasoline. While the hackers did move around within the company's information technology network, there wasn't any indication they were able to breach the more critical operational technology systems, he said.

It was only after Mandiant and Colonial were able to conclusively determine that the attack had been contained that they considered re-opening their pipeline, said Blount.

Colonial paid the hackers, who were an affiliate of a Russia-linked cybercrime group known as DarkSide, a $4.4 million ransom shortly after the hack. The hackers also stole nearly 100 gigabytes of data from Colonial Pipeline and threatened to leak it if the ransom wasn't paid, Bloomberg News reported last month.

Colonial has hired Rob Lee, the founder and chief executive officer of the Dragos Inc., a cybersecurity firm that focuses on industrial control systems, and John Strand, owner and security analyst at Black Hills Information Security, to consult on its cyber defenses and to focus on warding off future attacks.

https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

Text B

MARRIOT DISCLOSES MASSIVE DATA BREACH AFFECTING UP TO 500 MILLION GUESTS

Marriott said Friday that hackers have had access to the reservation systems of many of its hotel chains for the past four years, a breach that exposed private details of up to 500 million customers while underscoring the sensitive nature of records showing where and when people travel — and with whom.

The breach of the reservation system for Marriott's Starwood subsidiaries was one of the largest in history, after two record-setting Yahoo hacks, and was particularly troubling for the nature of the data that apparently was stolen, security experts said. That includes familiar information — such as names, addresses, credit card numbers and phone numbers — and also rarer prizes for hackers, such as passport numbers, travel locations and arrival and departure dates.

The potential value of such information on such a large percentage of the world's travelers triggered speculation that Marriott may have been the target of nation-state hackers seeking to track the movements of diplomats, spies, military officials and business executives. Yet even if the hackers were mere criminals in search of profit, such data offered the raw material for a range of possible misdeeds, including identity theft.

"This is extraordinarily intimate data," said Edward Hasbrouck, a San Francisco-based travel writer and consumer advocate who has long warned about the sensitivity and poor security of computerized travel records. "The travel industry has been grossly negligent compared to many industries when it comes to data privacy and security."

An unauthorized party accessed the reservation database of Starwood properties — which includes hotel chains St. Regis, Westin, Sheraton, Aloft, Le Meridien, Four Points and W Hotels — from 2014 onward, according to a Marriott news release. It acquired Starwood in 2016 and kept the reservation databases separate from its own until recently. The reservation system of Marriott hotels themselves were not affected by the breach reported Friday.

"We deeply regret this incident happened," Arne M. Sorenson, Marriott's chief executive, said in the news release. "We fell short of what our guests deserve and what we expect of ourselves. We are doing everything we can to support our guests, and using lessons learned to be better moving forward."

Marriott International is based in Bethesda, Md., and has more than 6,700 properties around the world. The company's shares were down nearly 6 percent Friday.

An internal security tool flagged the unauthorized party's activity on September 8. Marriott then discovered that the hackers had accessed the information, encrypted it and attempted to remove it. It took Marriott until late November to decrypt the information.

"It's not just that it's been continuing for four years, but that there were significant opportunities for higher scrutiny," said Paige Boshell, an attorney with Alabama-based Privacy Counsel LLC who advises on cyber risk management and response.

The news release specified that the company used encryption to protect credit card numbers. But Connie Kim, a Marriott spokeswoman, declined to comment on whether other personally identifiable information — including names, addresses, phone numbers, email addresses and passport numbers — was protected in this way, as security experts recommend.

The company acknowledged, however, a possible failing in the encryption security it had for credit card numbers, saying that it could not "rule out the possibility" that encryption keys were taken by hackers, allowing access to troves of valuable payment data. The most secure systems lock up data with encryption keys and also make sure those keys are stored safely.

"The fact that they can't rule out that the keys were taken sounds like a problem," said Matthew D. Green, a Johns Hopkins University cryptographer.

It's not the first time Starwood has been hacked. In 2015, Starwood, along with other luxury hotel brands such as Trump Hotels and Mandarin Oriental, fell prey to credit card breaches. Malware aimed at stealing credit and debit card information was found on payment systems at restaurants and stores in 54 Starwood hotels in North America, according to a 2016 online letter from company president Sergio D. Rivera. That breach happened just days after the Marriott acquisition was announced.

Cybersecurity experts on Friday debated whether the hackers likely were criminals collecting data for identity theft or nation-state spies collecting information on travelers worldwide. Hotel chains, with their vast customer databases and proprietary WiFi networks, can make appealing targets.

"We know that the hospitality business is a very attractive target for nation-states," said Thomas Rid, a political science professor at the Johns Hopkins School of Advanced International Studies who specializes in cybersecurity issues. "You can more easily hack some high-value targets from within a hotel WiFi."

The presence of passport numbers in data accessed by hackers is unusual for even a large breach, but such information is routinely collected by hotels in many countries, especially from international travelers. A passport number is not enough, by itself, to make a credible fake passport that could fool border agents or other government

security officials, but it's yet another piece of useful data for a criminal attempting identity theft.

The U.S. State Department issued a statement following reports of the breach Friday, "We are aware that some individuals' passport numbers may have been disclosed, but would like to emphasize that none of the U.S. Department of State's records or IT systems connect to Marriott's records or systems. No one can access the Department's records or obtain copies of a U.S. citizen's records by using a passport number."

Large amounts of travel data went online several decades ago, long before many other kinds of sensitive records, through computerized airline ticketing and hotel reservation systems, but the travel industry has lagged behind some others in adopting advanced forms of security, privacy advocates say.

Health and some other categories of information are singled out for specific protections under federal law. But travel data is not, even though it can paint a precise picture of a person's movements, lifestyle and relationships — down to whether two people traveling together choose one bed or two as they travel. Reservation systems also can provide advanced notice of where somebody is traveling, which could provide crucial political, military or business intelligence.

Security expert Matt Tait, a former British intelligence officer, said it was unclear whether the hackers were spies or mere criminals, though he suspected Marriott was a victim of a nation-state attack because the access lasted for so long without triggering suspicion.

"Nation-states are happy to watch and use the information very passively while criminals want to turn it into cash," said Tait, a senior cybersecurity fellow at the Robert S. Strauss Center for International Security and Law at the University of Texas at Austin.

Gary Leff, author of the View From the Wing blog, said that there have been numerous hacks in recent years in the travel industry and that information from rewards programs regularly gets bought and sold by criminals online. He expressed skepticism that the Starwood reservation system hack came from a foreign intelligence service.

"I don't think it necessarily would have taken a nation-state to crack into Starwood IT," said Leff.

Government officials on Friday called for stricter enforcement in consumer data privacy. New York Attorney General Barbara Underwood, Maryland Attorney General Brian Frosh and Pennsylvania Attorney General Josh Shapiro all said their offices had opened investigations into the Marriott breach.

https://www.washingtonpost.com/business/2018/11/30/marriott-discloses-massive-data-breach-impacting-million-guests/

b. The groups are re-mixed. Now each expert has to teach his new group his knowledge on the topic. After exchanging the information, be ready to answer the questions.

GRAMMAR

Exercise 82

Study grammar rules on the use of REPORTED SPEECH (see GRAMMAR REFERENCE pp. 174-177). Find 5 examples of both direct and indirect speech in two texts from the previous exercise. Transform them into their opposites (direct speech into indirect, indirect into direct).

Exercise 83

a. Look at the examples of direct speech and their indirect counterparts below. Choose the correct variant in indirect sentences.

1. Frank Abignale said, "Hackers don't cause breaches, people do". – Frank Abignale said that hackers *did not cause/had not caused* breaches.
2. Tom Kellermann explained, "The hacker underground has developed various weapons in the cyberspace that allow them to bypass the encryption". – Tom Kellermann explained that the hacker underground *had developed/developed* various weapons in the cyberspace that allow them to bypass the encryption
3. A programmer explained, "There are many devices which can be used for hacking". – A programmer explained that there *are/were* many devices which can be used for hacking
4. The policeman told the reporters, "Alberto Gonzales would drive through Miami shopping districts, hacking into stores' wireless networks" – The policeman told the reporters that Alberto Gonzales *would drive/drove* through Miami shopping districts, hacking into stores' wireless networks
5. A security specialist assumed, "Credit cards are more secure way to pay for the goods" – A security specialist assumed that credit cards *have been/were* more secure way to pay for the goods.

6. The CSO promises, "I'll keep the data safe!" – The CSO promises that *I/he* will keep the data safe!
7. The Commissioner reported, "The hacker sold the stolen credit card details on to Eastern European cyber criminals". – The Commissioner reported that the hacker *had sold\sold* the stolen credit card details on to Eastern European cyber criminals.
8. The expert explained, "His identity was stolen because of providing too much personal information on his social media" – The expert explained that his identity *has been/had been* stolen because of providing too much personal information on his social media.
9. He said, "Raspberry Pi is a computer which is extremely popular with hackers nowadays". – He said that Raspberry Pi *is/was* extremely popular with hackers nowadays.
10. The article says, "The amount of cyber crimes has increased over the past decade" – The article says the amount of cyber crimes had increased/increased over the past decade.

b. Put the words into the correct order.

1. Is service or website wonder punishable misuse whether I abuse this on of ?/.
2. Violation copyright a that law there if is prohibits he asks ?/.
3.So cyber this is campaign spreading rapidly extortion ?/.
4. Be guest the computer simple hacked questioned USB-cable his whether presenter a TV can a with ?/.
5. System still that does vulnerability exist ?/.
6. Social engineering powerful they asked for most the what tool was ?/.
7. Bug through much have how program the received the researchers bounty ?/.
8. Crimes negative the of impact is what computer ?/.
9. Infiltration illegal are what we avoid asking journalists the into us constantly do system to ?/.
10. There of how computer are viruses types many ?/.

Exercise 84

Transform direct statements, questions and order into indirect speech.

1. James Comey reported, "The investigation began as a referral from the Intelligence Community Inspector General"

2. The Comissioner told the computer forensics team, "Search for any evidence you can find on these servers".

3. The company's CSO told the reporters, "We have also investigated to determine whether there is evidence of computer intrusion".

4. The LAPD officer says, "And, of course, in addition to our technical work, we interviewed many people, involved in setting up and maintaining the various iterations of the defendant's personal server".

5. The magazine's reporter wondered, "Are there any traces of the illegal breach into computer system of the nuclear station?".

6. The digital forensics specialist said, "I should add here that we found no evidence that any of the additional work-related e-mails were intentionally deleted in an effort to conceal them".

7. "Is it a virus or a Trojan?", he inquired politely.

8. The security department recommends the company's employers, "Do not use WhatsApp for work-related communication".

9. John asked, "How can I hack the target form within a hotel Wi-Fi?"

10. Students asked, "Who is the first person convicted under the 1986 Computer Fraud and Abuse Act".

Exercise 85

Translate the sentences from Russian into English.

1. Лектор объяснил, что незаконное проникновение в компьютерную систему является уголовно наказуемым деянием.

2. Прокурор поинтересовался, было ли деяние совершенно со злым умыслом или по грубой неосторожности.

3. Начальник службы «Яндекс» сказал репортерам, что скомпрометированная учетная запись не имела доступа к внутренним серверам компании.

4. Исследователь задается вопросом, что же такое компьютерное пиратство.

5. Представитель корпорации Hyatt Hotels доложил, что они запустили программу для охотников за уязвимостями, которая позволяет этичным хакерами тестировать сайт компании и ее мобильное приложение.

6. Юрист объяснил, что в США существует три уровня секретности: «конфиденциально» (Confidential), «секретно» (Secret), «совершенно секретно» (Top Secret).

7. Джон всегда хотел пойти в полицию, поэтому он спросил, как можно стать специалистов в области цифровой криминалистике.
8. Полиция предупреждает, что люди с ограниченными возможностями часто становятся жертвами мошенников.
9. Граждане страны спрашивают, было ли небрежное обращение с секретными данными намеренным или нет.
10. Адвокат сказал ей, что при нарушении авторских прав, у компании будет достаточно денег, чтобы засудить ее.

LISTENING II

Exercise 86

Watch the Youtube video about digital forensics at https://www.youtube.com/watch?v=ZUqzcQc_syE and do the exercises.

a. BEFORE YOU WATCH. Look at the definition of 'forensics' taken from Cambridge Online Dictionary below and try to guess and explain what digital forensics is and what things it deals with.

Forensics – scientific methods of solving crimes, that involve examining objects or substances related to a crime.

b. WHILE YOU WATCH.

1. Watch the video and fill in the gaps in the sentences.

1. It is important for cyber security professionals to undergo a thorough process of _____, _____, _____, and _____ digital evidence.
2. To support this new discipline specialized tools have also emerged to assist investigators in the _____, _____, and _____ of evidence that might arise during the course of investigating.
3. Forensic analysts must make sure to analyze _____, _____ and _____, _____ and _____ to locate the point of compromise.
4. This eight-step process covers the entire _____ from data collection to examination and analysis to reporting.
5. Since investigators may be required to present evidence as part of _____, using this scientific process increases the likelihood that any evidence found will be fully admissible in a _____.

6. Another important consideration for organizations should they be the victim of a breach is the possible _____ by untrained staff.
7. Computer systems, networks, and mobile devices can all be _____ or _____ a cyber attack.
8. Computer forensics may rely on the need to create _____ to preserve evidence or virtual drives may be used to emulate an entire machine.
9. For example in situations where card holder data is involved as well as the decision to involve outside specialists when you discover that your enterprise _____.
10. Without digital forensics evidence can go _____ or become _____ and systems may remain vulnerable to additional attacks.

2. Watch the video once again and answer the questions.

1. What does the work of digital forensics specialist involve?
2. What helped shape digital forensic methods into what they are today?
3. What types of cyber crimes are distinguished in the video? What crimes do these types include?
4. What is digital forensics scientific process? How many phases does it include? What do they include?
5. What do the organisations do to mitigate the risk of mishandling the evidences?
6. What are the three distinct branches of digital forensics?
7. Why does mobile devices forensics present its own unique challenges?
8. What should the enterprise cybersecurity program have?

c. AFTER YOU WATCH. Discuss with your group mates the content of the video. What do you think of the job of digital forensics specialist? What is the most important things in their job?

SPEAKING II

Exercise 87

Round Table Discussion

a. Read the brief background of Van Buren vs. United States case.

Following years of consternation, the US legal landscape appears to have tilted decisively in favor of ethical hackers, as a recent Supreme Court decision effectively

narrows the scope of what constitutes 'unauthorized access' under the Computer Fraud and Abuse Act (CFAA).

Most concerns focus on the law's scope, with critics arguing that the CFAA has been extended beyond far beyond policymakers' original objectives when they laid them out more than three decades ago.

Concerns about the CFAA have centered mostly around the way the act makes use of a computer "without authorization" a criminal offence.

Given that there is no accompanying definition of what "authorization" entails, this raises the specter of computer users inadvertently breaking federal law for things like using an application in a way that breaches its license agreement.

And the act's broad provisions makes huge swathes of computer security work, including ethical hacking, penetration testing, and participating in bug bounty programs, fraught with legal risk.

But a fresh decision in the Supreme Court relating to *Van Buren vs. United States* limits the act's scope in a way that could make work of cybersecurity professionals (i.e. researches whose work often involves accessing computer systems in ways that violate terms of service or other policies) easier and less anxiety-inducing.

https://portswigger.net/daily-swig/us-computer-fraud-and-abuse-act-what-the-landmark-van-buren-ruling-means-for-security-researchers

b. Internet Activity. Now, when you are aware of the background, get acquainted with the details of the case (https://epic.org/documents/van-buren-v-united-states/) and watch the video where two lawyers discuss the impact of the case on the US legal landscape (https://www.youtube.com/watch?v=23va1vj41Zc).

c. Discuss with your group mates that impact of the case. Is it a real milestone in legislation? What do think of work of cybersecurity researchers, bug bounty hunters and so-called 'white hats'? Should it be restricted by the law? Give your own assessment from the legal perspective.

TRANSLATION PRACTICE

Exercise 88

Read the text and translate it from English into Russian.

UBER RESPONDING TO ‘CYBERSECURITY INCIDENT AFTER HACK

Uber has been hacked in an attack that appears to have breached the ride-hailing company’s internal systems.

The California-based company confirmed it was responding to a “cybersecurity incident”, after the New York Times reported that a hack had accessed the company’s network and forced it to take several internal communications and engineering systems offline. The hacker claimed to be 18 years old, according to the report.

Uber confirmed that there are no issues with the company’s service, which operates in more than 10,000 cities around the world.

A hacker compromised the employee workplace messaging app Slack and used it to send a message to Uber employees announcing that it had suffered a data breach.

Sam Curry, a senior engineer at non-fungible token creator Yuga Labs, said he was contacted by the Uber hacker on the HackerOne platform and had been shown “very convincing” screenshots of full administrative access to Uber’s cloud services.

“From my understanding, the attacker had keys to the kingdom after obtaining an internal file with credentials to nearly everything,” Curry told the Guardian. He added: “Based on the screenshots and my understanding of the hack, they likely had access to read/modify the cloud services which run Uber and store user information.”

The company has been hacked before. Its former chief security officer, Joseph Sullivan, is on trial on allegations he arranged to pay hackers $100,000 as part of an attempt to cover up a 2016 attack in which the personal information of about 57 million customers and drivers was stolen.

It appeared the hacker was able to gain access to other internal company systems, posting an explicit photo on an internal information page for employees, according to the New York Times. “We are in touch with law enforcement and will post additional updates here as they become available,” Uber said in the tweet confirming the attack.

The Slack system was taken offline on Thursday afternoon by Uber after employees received the message from the hacker.

“I announce I am a hacker and Uber has suffered a data breach,” the message read, going on to list several internal databases that were claimed to be compromised, the report added.

The New York Times reported that the person who claimed responsibility for the hack said they gained access through social engineering, a term for tricking an employee into granting access.

The hacker sent a text message to an Uber worker claiming to be a company tech employee and persuaded the worker to hand over a password that gave them access to

the network. The hacker, who had provided a Telegram account address, said they broke in because the company had weak security, according to the report.

Staff at the company were instructed to not use Slack. Other internal systems, too, were reportedly inaccessible.

https://www.theguardian.com/technology/2022/sep/15/uber-computer-network-hack-report

WRITING

Exercise 89

Writing an abstract

Watch the video at https://www.youtube.com/watch?v=lbCh94nJqIo&t=1s about how to write a clear abstract and answer the questions.

1. What is a typical volume of an abstract?
2. Where does an abstract come in dissertations and theses?
3. What four things should be included?
4. Which section should be written in the past simple tense?
5. How can readers assess the credibility and generalizability of the work?
6. What is the purpose of key words?

Exercise 90

Look at the abstract to the article *'Cybercrime Legislation in the Netherlands'* by Prof. Bert-Jaap Koops and highlight the elements mentioned in the previous exercise. How can you assess the abstract?

This report, written for the 18th International Congress on Comparative Law of July 2010, comprehensively discusses cybercrime legislation and case-law in the Netherlands. Following the structure of the Cybercrime Convention, it first describes substantive criminal law: core cybercrimes such as hacking, viruses, denial-of-service attacks, and misuse of devices; computer-related traditional offences such as fraud and forgery; content-related crimes such as child pornography and racism; and copyright infringement. It also goes into crimes not covered by the Cybercrime Convention: data theft (can virtual goods be stolen?), identity theft, grooming, privacy and data protection offences, and ISP liability. Second, investigation powers are discussed, such

as production and preservation orders, computer search and seizure, traffic data and data retention, and communications interception. Third, computer-related evidence and jurisdiction issues are briefly discussed, as well as self-regulatory initiatives for notice-and-takedown and filtering and blocking systems. The report then reflects on the way international legal instruments have been implemented in Dutch law, pointing out omissions in criminalisation as well as some provisions that have fundamentally affected the legal system. The report concludes with identifying issues for comparative legal research and for further harmonisation at the international level.

B.J. Koops, Cybercrime Legislation in the Netherlands // NETHERLANDS REPORTS TO THE EIGHTEENTH INTERNATIONAL CONGRESS OF COMPARATIVE LAW, pp. 595-633

Exercise 91

Use the link and read the article. Write an abstract to it. Which keywords can be highlighted?

Cláudia Fernandes, Steganography and Computer Forensics -the art of hiding information: a systematic review – https://aris-journal.com/aris/index.php/journal/article/view/20/16

TEST 3.
THE COMPUTER'S ROLE IN CRIME

Choose the correct word(s) to complete the sentences:

1. A person who is responsible for overseeing the company's and information security is a _____.
a) chief executive officer;
b) chief security officer;
c) bug bounty hunter;
d) digital forensics specialist.

2. The psychological manipulation which has the target to get confidential information is _____.
a) social engineering;
b) scamming;
c) Internet manipulation;
d) compromising.

3. The reporter asked, "Are there any dangerous vulnerabilities in this system?" – The reporter asked...
a) if there are any dangerous vulnerabilities in that system;
b) were there any dangerous vulnerabilities in that system;
c) if there were any dangerous vulnerabilities in this system;
d) if there were any dangerous vulnerabilities in that system.

4. Accessing a computer without proper authorization and gaining some financial information from any protected computer is _____.
a) social engineering;
b) computer trespass;
c) scamming;
d) embezzlement.

5. The study said, "Global economic recession has a serious impact on software piracy". – The study said that global economic recession _____ a serious impact on software piracy.
a) can have;
b) had;

c) has;
d) has had.

6. A deal offered by organizations and software developers by which programmers can get money compensation for finding bugs and vulnerabilities is _____.
a) bugs search program;
b) ethical security program;
c) bug bounty program;
d) cyber security program.

7. A program which seems useful but designed to be harmful is _____.
a) a Trojan horse;
b) a virus;
c) an antivirus program;
d) a logic bomb.

8. Consumers choose the same password for multiple services far too often, _____ their data.
a) compromised;
b) misusing;
c) compromising;
d) scammed.

9. Alon Gal said, "This database is going to be used by hackers, political hacktivists and of course governments to harm our privacy even further" – Alon Gal said _____ database _____ be used by hackers, political hacktivists and of course governments to harm our privacy even further.
a) if; will be going to;
b) that; is going to;
c) whether; was going to;
d) that; was going to.

10. A highly skilled hacker was able to _____ the company's servers and steal financial information.
a) compromise;
b) infiltrate;
c) extort;
d) misuse.

11. The official demonstrated _____ negligence in handling sensitive information.
a) gross;
b) strong;
c) heavy;
d) severe.

12. Digital forensics expert was asked, "Was the video created using a new generation of artificial intelligence tools" – Digital forensics expert was asked _____ using a new generation of artificial intelligence tools.
a) that the video had been created;
b) if had the video been created;
c) whether was the video created;
d) if the video had been created.

13. He said, "Tinley planted a logic bomb in the spreadsheet software provided to Siemens two weeks ago" – He said that Tinley _____ a logic bomb in the spreadsheet software provided to Siemens two weeks _____.
a) had planted, before;
b) has planted, ago;
c) had planted, ago;
d) planted, before.

14. Chinese leaders have pledged to crack down on software _____.
a) compromising;
b) misusing;
c) piracy;
d) conspiracy.

15. One user in Reddit's social engineering thread wonders, "Are most 'hackers' these days just glorified social engineers with programming skills?" – One user in Reddit's social engineering thread wonders _____ most 'hackers' _____ days _____ just glorified social engineers with programming skills.
a) whether, those, were;
b) whether, these, are;
c) that, these, are;
d) that, these, were.

Unit 4.
People in Cybercrime

LEAD-IN

Work in pairs and explain how you understand this quotation:

"For every lock, there is someone out there trying to pick it or break in"

by David Bernstein

Do you agree with the statement below? Explain your opinion:

"You can't defend. You can't prevent. The only thing you can do is detect and respond"

by Bruce Schneier

KEY TERMS

a cybercrime investigator	следователь по делам о преступлениях в сфере IT
to investigate	расследовать
an investigation	расследование
a cybercriminal	преступник, виновный в совершении преступления в сфере IT
a cybercriminal gang	банда киберпреступников
a cyberintruder	хакер
a cyberfraud	кибермошенничество
a hacker	хакер
a hacker attack	хакерская атака
to hack	взламывать
to be hacked	быть взломанным
to foil	предотвращать
ransomware	вирус-вымогатель

to be resilient against	быть устойчивым к
a victim	жертва
a forensic evidence	судебное доказательство
to takedown someone	ликвидировать (например, преступника)
to put someone behind bars	посадить кого-либо за решетку
malicious	злоумышленный, вредоносный
a malefactor	злоумышленник
to close a case	закрыть дело, закончить расследование
an encryption	шифрование
a decryption key	ключ шифрования
a malware	вредоносная программа
a data breach	утечка данных
a white-hat hacker	этичный хакер
a black-hat hacker	хакер-злоумышленник

Exercise 92

a. What parts of speech are the following words:

malware, malefactor, malicious, takedown, victim, resilient, encryption, hack, hacker, investigator, investigate, investigative, investigation, data, cybercriminal, cybercrime.

b. Identify roots, stems, suffixes and translate the words.

Exercise 93

Which word is odd?

cybercrime	cyberfraud	hacker attack	theft
look into	investigate	prosecute	punish
foil	protect	avoid	prevent
benefactor	attacker	malefactor	intruder
evil	malicious	dangerous	vicious
viable	sustainable	sophisticated	resilient
clue	evidence	proof	tool

Exercise 94

a. Match the words with similar meaning:

1) investigate	a) prevent
2) malicious	b) solve a crime
3) close a case	c) vicious
4) resilient	d) bloatware
5) encryption	e) inquire into
6) malware	f) strong
7) foil	g) encoding

b. Match the words with opposite meaning:

1) victim	a) cybercrime investigator
2) malware	b) malicious
3) black-hat hacker	c) criminal
4) malefactor	d) white-hat hacker
5) data breach	e) software
6) benevolent	f) benefactor
7) cybercriminal	g) data protection

Exercise 95

Find 11 words:

V	X	E	D	Y	Y	W	R	O	I	Q	M
I	D	Z	K	U	C	F	A	P	N	E	A
C	F	K	O	K	Y	G	N	O	V	W	L
T	A	Y	O	Q	B	Q	S	L	E	T	E
I	M	V	B	H	E	N	O	M	S	R	F
M	A	L	W	A	R	E	M	E	T	Y	A
Q	L	M	N	C	C	A	W	V	I	U	C
A	I	A	Z	K	R	Z	A	I	G	I	T
Z	C	E	P	E	I	Q	R	D	A	O	O
X	I	C	J	R	M	E	E	E	T	P	R
F	O	I	L	P	I	N	O	N	O	X	G
C	U	P	H	X	N	U	V	C	R	U	D
D	S	G	T	E	A	H	I	E	Z	Z	K
V	R	E	S	I	L	I	E	N	T	I	Z

Exercise 96

Match the words to the definitions:

1) hacker	a) software designed by criminals to prevent computer users from getting access to their own computer system unless they pay money
2) victim	b) a person who gets into computer systems without permission, but has morally good reasons for doing this
3) cybercrime investigator	c) software that is designed to damage the way a computer works
4) malware	d) a person who has suffered the effects of cybercrime
5) ransomware	e) a person whose job is to examine a cybercrime in order to find a criminal
6) resilient	f) an occasion when private information can be seen by people who should not be able to see it
7) data breach	g) someone who gets into other people's computer systems without permission in order to find out information or to do something illegal
8) white-hat hacker	h) able to return quickly to a previous good condition after problems

Exercise 97

a. Match the word combinations:

1) to investigate	a) gang
2) a cybercrime	b) behind bars
3) data	c) evidence
4) a cybercriminal	d) investigator
5) to put someone	e) key

6) a forensic
7) an encryption
f) breach
g) a cybercrime

b. Complete the following sentences using the words and word combinations from the previous tasks (the first letter is given in brackets):

1. The criminals did not complain of any unlawful methods applied during the i_____.
2. This company has a high level of security, for all the time not a single h_____ was successful.
3. Unfortunately, my twitter account was h_____ in the last days.
4. Organized c_____ brought down by international police cooperation, says Europol: five members of an international organised c_____ group have been arrested.
5. For 10 years the cybercrime gang have attempted to attack banks, e-payment systems and financial institutions using pieces of m_____ they designed, known as Carbanak and Cobalt.
6. Undoubtedly r_____ is still the absolute king of cybercrime, even though we have seen a striking evolution.
7. Two officers of the Russian Federal Security Service (FSB) and a cybercrime i_____ from Kaspersky Lab have reportedly been charged with treason for helping U.S. intelligence services.
8. Most people think of any m_____ software as a virus, even though it is technically inaccurate.
9. Companies need to be more r_____ against cybercrimes like ransomware and phishing.
10. Both the police and cybercrime investigators immediately took necessary measures to f_____ the attempt.

Exercise 98

Translate these sentences from Russian into English using the words and word combinations from the previous tasks:

1) Банда киберпреступников была отправлена за решетку на прошлой неделе.
2) Вирусы-вымогатели и другие вредоносные программы создают множество проблем в сфере информационных технологий.

3) Джулиан Ассанж считается одним из самых влиятельных хакеров в истории киберпреступности.
4) Следователи по киберпреступлениям помогают предотвращать хакерские атаки.
5) Наша компания стала жертвой хакеров: система безопасности была взломана, поэтому произошла утечка данных.
6) Банда киберпреступников недавно разработала новое вредоносное ПО.
7) Злоумышленники попытались взломать мой компьютер, но я вовремя обратился за помощью к следователю по киберпреступлениям.
8) «Этичные» хакеры специализируются на тестировании безопасности компьютерных систем.
9) Компания «Яндекс» отказалась передать ФСБ ключи шифрования.
10) Вирусы-вымогатели являются разновидностью кибер-мошенничества.

Exercise 99

Work in pairs. Discuss the questions:

1. What does the job of a cybercrime investigator include?
2. Who helps them to solve crimes?
3. What types of malwares exist?
4. How to stay resilient against cybercrimes?

READING I

Exercise 100

Read the first fragment of an interview with Catalin Cosoi. What does his job involve?

FOILING CYBERCRIMES AROUND THE WORLD

To help organizations and individuals understand how to better protect themselves and become more resilient against cyber threats like ransomware, we spoke with Catalin Cosoi, Senior Director, Investigations and Forensics at Bitdefender. As a ransomware expert and cybersecurity investigator, Catalin is one of the many cybersecurity heroes working behind the scenes at Bitdefender to not only make our solutions and services better, but also stop cybercrime in its tracks. Catalin and his team work closely with law enforcement agencies around the world – including Interpol, Europol and the FBI – to investigate cybercrimes, help victims recover from cyber-attacks, and put cybercriminal gangs behind bars.

What is a cybercrime investigator and what do you do?

Catalin: As a cybercrime investigator, I am expected to analyze the computer systems of people or organizations that have been the victim of cyber-attacks, gathering evidence and helping them recover data, repair their systems and prevent such an attack from happening again. Several years ago, our Investigations and Forensics team at Bitdefender began building close relationships with law enforcement agencies, to assist them in their pursuit of cybercriminals. We recognized that the cyber forensic evidence we recover from our clients could aid law enforcement in their efforts to takedown cybercriminal gangs and put their members behind bars.

Today, we often work in tandem with law enforcement. Because we at Bitdefender protect hundreds of millions of customer endpoints around the world and process billions of malicious samples daily, we have a huge pool of data to draw from. We're able to recognize trends and connect dots that a single law enforcement agency working a specific case may not be aware of. For example, we can often recognize the modus operandi that is indicative of a particular cybercriminal gang, or we might be able to trace a cyber-attack back to a particular IP address, which we then share with law enforcement so they can investigate it further or identify the owner. And, because cybercrime isn't contained within the borders of any one country, we often end up working with numerous law enforcement agencies in multiple countries over the course of an investigation until the case is closed.

At the same time, we help our clients to recover any stolen or encrypted files or data, clean up their systems and better secure their systems from future threats. The intelligence we learn from each investigation gets applied to all our clients, so we're

able to better protect them all against the latest threats, no matter where in the world they're originating.

https://businessinsights.bitdefender.com/foiling-cybercrime-around-the-world-an-interview-with-a-cybercrime-investigator

Notes:

Interpol – (англ. International Criminal Police Organization, ICPO) международная организация, основной задачей которой является объединение усилий национальных правоохранительных органов в области борьбы с уголовной преступностью

Europol – полицейская служба Европейского союза, расположенная в Гааге

Law enforcement agencies – правоохранительные органы

Exercise 101

Decide if the statements are true or false. Correct the false statements.

STATEMENT	**TRUE**	**FALSE**
1. Catalin and his team have no connections with law enforcement agencies.		
2. He rarely studies the computer systems of people or organizations that have been the victim of cyber-attacks.		
3. Bitdefender helps people to recover their stolen data.		
4. Bitdefender includes such teams as Investigations and Developers.		
5. Forensic evidence recovered from Bitdefender's clients could help law enforcement in their efforts to takedown cybercriminal gangs.		
6. Bitdefender has a moderate pool of data to draw from.		
7. Investigators are always able to trace a cyber-attack back to a particular IP address.		
8. Usually cybercrimes aren't contained within the borders of any one country.		
9. Bitdefender's team relies on the experience of previous investigations to better protect its clients against the latest threats.		

Exercise 102

Find in the text the derivatives of the words:

Cyber, investigate, enforce, malice, day, indicate, steal, apply, late.

Exercise 103

Find in the text and translate the sentences which contain:

Present Tenses (active), Modal Verbs, Complex Object, Infinitive.

Exercise 104

Complete or finish the following sentences:

1. Catalin is one of the many cybersecurity heroes working behind the scenes at Bitdefender to …
2. Catalin and his team work closely with law enforcement agencies around the world – including … – to investigate cybercrimes, …
3. As a cybercrime investigator, I am expected to … of people or organizations that …, gathering evidence and helping them recover data, repair their … and prevent …
4. We recognized that the cyber forensic evidence we recover from our clients could … in their efforts to …
5. Today, we often work in …
6. We might be able to …, which we then share with law enforcement so they can …
7. At the same time, we're helping our clients …, clean up their systems and better secure their systems from …
8. We're able to better protect them all against the latest threats, …

Exercise 105

a. Look through the short fragments about cybercrime investigation related matters and complete them with the words and word combinations in the box:

tools decryption keys data cybercriminals ransomware industries encryption malware law enforcement agencies investigate risks victim

1. _____ has become incredibly widespread. Over the past five years, we've seen attacks of great force impact important organizations in critical _____. At Bitdefender, we actively monitor the main groups of ransomware. Whether it's ransomware as a service (RaaS) or custom-made ransomware, we observe and watch for methods we can combat the attack.

2. _____ are human, so they do make mistakes. Sometimes we find mistakes in the implementation of the _____ itself. More often, we find pieces of information that give us clues to where the _____ may be stored.

3. Bitdefender provides _____ the information as to where the decryption keys may be stored in that infrastructure. They_____, and if they're able to find the decryption keys, they bring them to us.

4. Bitdefender employees believe that it's very important to provide ransomware decryption _____ to the public for free. The benefits far outweigh the _____.

5. If you've been the _____ of a ransomware attack, Bitdefender employees highly recommend you start by searching nomoreransom.org. You can often type in the name of the _____ that has infected your systems and find a free decryption tool to help you recover your _____.

Exercise 106

Read the text and match the headings to the paragraphs:

1. Three best practices	a. For our clients, cyber resiliency means being able to prevent or cope with any type of cyber-attack, whether its ransomware, a data breach, a hacker accessing your computer, or anything else. These days, it's not a matter of if you will be attacked, but a matter of when. So, everyone must be prepared. They must be resilient.
2. Resiliency: meaning	b. In the case of ransomware, that means you should have backups in place so you can bring back your infrastructure after an attack. Make backups of anything important to you, and keep those backups stored on an unconnected, external hard drive. For many people, this means their family photos and

	important personal documents. Make a new backup copy every month.
3. Two things to keep your employees alert	c. Always pay attention to what you're doing. As an individual, be aware of what links you're clicking on and whether they are trustworthy. When it comes to organizations, most breaches are caused by an employee making a mistake.
4. The importance of making backups	d. Cybersecurity awareness and training programs are critical for keeping employees alert to risks and helping ensure they don't make a mistake that could lead to a major incident.
5. Being careful	e. October is cybersecurity awareness month, so I always recommend people to revisit these three best practices each October: ensure your backups are occurring properly, check your security solutions, and refresh your cybersecurity training to ensure you're on top of your game.

Exercise 107

Answer the questions:

1. What practices of preventing ransomware attacks are enumerated in the text?
2. When is cybersecurity awareness month?
3. Why is it important to make backups?
4. Who causes data breaches?
5. Where should you store your backups?
6. Is it likely that a person will be attacked one day?

GRAMMAR

Exercise 108

Analyze the underlined structure in the text from Exercise 15. How is it called? What parts does it consist of? Study grammar rules on the use of COMPLEX OBJECT (see GRAMMAR REFERENCE p. 177-178).

Exercise 109

Translate the sentences into Russian paying attention to the infinitive and participle structures:

1. Experts believe cyber-attacks to start soon.
2. We expect our cybercrime investigators to do their work professionally.
3. The investigators found the system to be hacked.
4. We noticed this hacker designing a brand-new ransomware.
5. The police let the cybercriminal gang go.
6. Many cybercrime investigators would like their clients to be more aware of the ransomware threat.
7. Cybercrime investigators made him confess.
8. Malefactors made the victim pay a huge sum of money.
9. Cybercriminals believe police to be absolutely helpless.
10. IT specialists heard this hacker be a white-hat.

Exercise 110

Complete the sentences…

1. We consider this malware to…
2. His employer wants him to…
3. The investigator expects this cybercrime to…
4. I wouldn't like my backups to…

Exercise 111

Put the verbs in brackets into correct form:

1. We want our law enforcement officials _____ (be) able to investigate and prosecute cybercrimes.
2. The Internet allows criminals _____ (make) money by committing fraud, theft, or even murder, all while remaining anonymous.
3. The police heard him _____ (leave) the country.
4. Law enforcement agencies made Bitdefender _____ (investigate) that case more deeply.
5. We expect our clients _____ (report) cybercrimes immediately.

6. Law enforcement agencies would like cybercrimes _____ (disappear).
7. Black-hat hackers ordered him _____ (sell) his car and house.
8. The employer expects us _____ (refresh) our cybersecurity training.

LISTENING I

Exercise 112

You are going to watch a video version of an interview with Catalin Cosoi at https://youtu.be/8CV1f6a9b-c

a. BEFORE YOU WATCH. Answer the questions:

1. What are the advantages of working in cybercrime investigation?
2. Have you ever been a victim of a cybercrime?
3. What should you do if hackers want you to pay them money?

b. WHILE YOU WATCH. Fill in the gaps:

Back in (1) _____ I was a student at (2) _____. During the summer vacation, we asked to work in (3) _____ for at least a month. So, I (4) _____ at Bitdefender. And once I got here, they offered me the possibility to work on (5) _____. I managed to apply for a (6) _____. Six (7) _____ later and a lot of (8) _____ that have been successfully closed and a lot of technologies that I personally (9) _____ now are in the (10) _____.

It's the perfect place to be for me. Day-to-day activities consist in to helping (11) _____ with their cyber investigations. Working together, we can actually go a bit further than just (12) _____ a threat. We can actually go closer to the (13) _____ and help law enforcement to put them behind bars.

To be built for (14) _____ means to have to work constantly evolving. And that means we are building today the (15) _____ that we will need tomorrow.

c. AFTER YOU WATCH. Answer the questions:

1. When did Catalin start working at Bitdefender?
2. What does he feel about his job?
3. How does he describe his day-to-day activities?
4. What are they “building”?

5. Would you like to work in a company such as Bitdefender? Why / why not?

READING II

Exercise 113

Match the words from the text with their definitions:

1) to exploit	a) an official document, signed by a judge or other person in authority, that gives the police permission to search someone's home, arrest a person
2) vulnerability	b) a file that gives you practical instructions on how to do something or how to use something
3) unauthorized	c) containing important new ideas that influence later developments
4) consumers	d) an uncontrolled situation in which people do what they want because there are no limits to stop them
5) an amateur hacker	e) a violent and forceful attack
6) an onslaught	f) the quality of being easily hurt, influenced, or attacked
7) free-for-all	g) a person who buys goods or services for their own use
8) seminal	h) to use someone or something unfairly for your own advantage
9) computer manuals	i) hacker who does not have much skill in what he does
10) warrant	j) not officially allowed

Exercise 114

Read the text:

HACKING AND HACKERS

Computer hacking is the act of identifying and exploiting system and network vulnerabilities in order to obtain unauthorized access to those systems. Not all hacking is malicious. White-hat hackers may work in cyber security or as software engineers and testers seeking out vulnerabilities in order to fix

them. Black-hat hackers operate with malicious intent. There is a large grey area populated by political activists and hackers who wear both hats.

Hacking costs companies and consumers trillions of dollars every year. According to CPO Magazine, by 2021, hacking attacks will cost a total $6 trillion, up from $2 trillion in losses reported in 2019. Much of the cybercrime problem stems from the same features of the internet from which we all benefit. Even the most amateur hacker can easily find all the tools they need online at no cost.

The hacker onslaught didn't occur overnight. It took decades of work by now-famous hackers to discover critical vulnerabilities and reveal the strategies that established the foundations of the internet and its free-for-all libertarianism.

A seminal figure in American hacking, Kevin Mitnick got his career start as a teen. In 1981, he was charged with stealing computer manuals from Pacific Bell. In 1982, he hacked the North American Defense Command (NORAD), an achievement that inspired the 1983 film War Games. In 1989, he hacked Digital Equipment Corporation's (DEC) network and made copies of their software. Because DEC was a leading computer manufacturer at the time, this act put Mitnick on the map. He was later arrested, convicted and sent to prison. During his conditional release, he hacked Pacific Bell's voicemail systems.

Throughout his hacking career, Mitnick never exploited the access and data he obtained. It's widely believed that he once obtained full control of Pacific Bell's network simply to prove it could be done. A warrant was issued for his arrest for the Pacific Bell incident, but Mitnick fled and lived in hiding for more than two years. When caught, he served time in prison for multiple counts of wire fraud and computer fraud. Although Mitnick ultimately went white hat, he may be part of the both-hats grey area.

https://www.kaspersky.com/resource-center/threats/top-ten-greatest-hackers

Notes:

Pacific Bell - телефонная компания, предоставляющая услуги связи в Калифорнии

North American Defense Command - командование воздушно-космической обороны Северной Америки

Digital Equipment Corporation - американская компьютерная компания, была основана в 1957 году Кеном Олсеном и Харланом Андерсоном

Exercise 115

Decide if the statements are true or false. Correct the false statements.

STATEMENT	TRUE	FALSE
1. Black-hat hackers usually operate with benevolent intent.		
2. According to CPO Magazine, by 2021, hacking onslaughts will cost a total $6 million, up from $4 billion in losses reported in 2019.		
3. Even the most unexperienced cybercriminal can easily find all the tools they need online free of charge.		
4. It takes hacker a little time to find vulnerabilities in the system.		
5. Kevin Mitnick wasn't an adult person when he started his career.		
6. His achievements inspired several novels.		
7. He has never been arrested.		
8. Mitnick managed to escape from the police and hide.		
9. Mitnick is a famous black-hat hacker.		

Exercise 116

Answer the questions on the text:

1. What is computer hacking?
2. What do white-hat hackers do?
3. Where does the cybercrime problem stem from?
4. When did Kevin Mitnick hack NORAD?
5. What act put Mitnick on the map?
6. Has he ever exploited the stolen data?

Exercise 117

Internet Activity

a. Group work. Study information about famous hackers:

Link for group A: Albert Gonzalez https://www.blackhatethicalhacking.com/articles/hacking-stories/albert-gonzalez-the-get-rich-or-die-trying-crew-who-stole-130-million-credit-card-numbers/

Link for group B: Kevin Poulsen https://www.blackhatethicalhacking.com/articles/hacking-stories/kevin-poulsen-dark-dante-and-his-hacking-activities-on-arpanets-networks/

b. Complete Personal Profiles of Albert Gonzalez (group A) and Kevin Poulsen (group B):

Group A:

Albert Gonzalez	Time and country of birth: First steps into hacking: Hacked companies / systems: Arrests, sentences: Activity in the recent years:

Group B:

	Time and country of birth: First steps into hacking: Hacked companies / systems: Arrests, sentences: Activity in the recent years:

c. Share the information you have found with your group. Be ready to present the story of your hacker relying on his Personal Profile.

Exercise 118

a. Jigsaw activity. Group work. The class is divided into 2 "expert" groups (A, B). Each group reads one of the texts below. For example, Group A reads Text "Operation OpRussia – Anonymous attacks on Russia", Group B reads Text "How do QR Codes work and how criminal hackers use them to generate phishing attacks". Then the groups are re-mixed. Now each expert has to teach his new group his knowledge on the topic. After exchanging the information, be ready to answer the questions.

TEXT A
OPERATION OPRUSSIA – ANONYMOUS ATTACKS ON RUSSIA

Originating in 2003 on 4chan, Anonymous is an international activist and hacktivist group and movement known for its various cyberattacks against several governments, government agencies, and corporations whose mission is to combat establishment hypocrisy and corruption.

In late 2021, anticipating the military build-up near the Russia-Ukraine border, they acted to propagate peace plans to end the war in Donbas (the armed conflict between Ukraine and Russia started in 2014) by defacing various government websites in China, as the United Nations Network on Migration website.

On February 24, 2022, 5 days after Vladimir Putin ordered the invasion of Ukraine, Twitter accounts associated with Anonymous declared that they will launch a 'cyber operation' called "OpRussia" against the Russian Federation.

A few hours after the Anonymous collective called to action against Russia, its member have taken down the website of Russian propaganda RT news and also attacked the servers of the Russian Defense Ministry. Anonymous hacked into Russian TV channels, featuring Ukrainian Music and national symbols. They also leaked 200GB of emails from the Belarusian weapons manufacturer Tetraedr, which provided logistical support for Russia.

Operation Russia has already raised global awareness of the dangers of being hacked. Those attacks can no longer be virtual consequences, as online hacking activities can now be linked with real-world effects. As the campaign continues it raises

questions about the possibility of similar attacks to other countries, or even worse attacks that may target nuclear power plants as Stuxnet did 12 years ago.

Ransomware attacks becoming more sophisticated than ever, targeting cloud backups, and servers which resulted in targets being unable to restore their data. All these come as a reminder of why organizations need more and continuous investing in cyber security technologies to better protect themselves against such attacks in the future.

https://www.blackhatethicalhacking.com/articles/operation-oprussia-anonymous-attacks-on-russia/

TEXT B

HOW DO QR CODES WORK AND HOW CRIMINAL HACKERS USE THEM TO GENERATE PHISHING ATTACKS

It's almost certain that we interact with some kind of barcode every day. QR codes are widely used in public and are almost all over the place, from advertisements, product packaging, bus stops, train stations, boarding passes, to WIFI hotspots, you get the picture. The main reason for the rise of QR codes is mainly because they're easy to create, easy to use and now almost any device with a camera is capable of reading them.

With all the upsides of using QR codes, there are some dangerous consequences when using them without knowing what a malicious actor can do to your device or personal data by just scanning a QR code.

Thanks to the vulnerabilities that lie in many of these proprietary scanning devices, it's possible for an attacker to exploit common vulnerabilities using a malicious payload packed into custom QR codes or even trick users using social engineering (phishing), like creating a malicious WIFI access point.

When a QR code is scanned, an attacker can easily embed a malicious URL containing custom malware which can lead to the compromise of the victim's data.

It's difficult to spot malicious QR codes before actually scanning them, so it's safe not to scan any QR code that you don't surely know what it does or what its purpose is.

Cyber-criminals will always use new methods to get confidential information or cause damage to organizations or individuals, by knowing more, or what a malicious QR code can do to your device could potentially be beneficial in the future to think twice before scanning one.

https://www.blackhatethicalhacking.com/articles/how-do-qr-codes-work-and-how-criminal-hackers-use-them-to-generate-phishing-attacks-demo/

b. Study some useful phrases for making a summary:

I am going to make a summary of the text…
The text is called…
The text is devoted to // is focused on …
At the beginning of the text the author…
The text says (underlines, stresses, highlights) that…
The text goes on to say (stress, explain, analyze) …
It is interesting to notice (note) …
In conclusion // Finally, the author…

c. Make a summary of the text you have read. Share information with other students.

Exercise 119

Internet Activity

a. Work in groups of three. Each student reads about one of the 25 most famous hackers at https://warbletoncouncil.org/hackers-famosos-1246

b. Share the information with your group. What were their cybercrimes?

READING III

Exercise 119

Read the text about a woman in cybercrime:

A WOMAN IN CYBERCRIME

Hackers have a lot of stereotypes. For example, most hackers are male or hackers don't care about their look and personality. There are many girl hackers in the world who can inspire the generation. The female hackers prove that girls aren't aspiring to be models or actresses, they can also become good coders and hackers.

Kristina Svechinskaya:

In 2011 Svechinskaya and 37 others hackers used fake bank accounts, fake passports and a Zeus Trojan to steal $3 million from U.S. banks and another $9 million British banks. Svechinskaya opened at least five accounts under her own name and under the names "Anastasia Opokina" and "Svetlana Makarova" at Bank of America and Wachovia, into which over $35,000 was fraudulently deposited, affecting three victims, and from which approximately $11,000 was successfully withdrawn.

Svechinskaya was reportedly included in the group for her connections to hacker culture and her ability to get a hold of fake passports. The team also prized her for her obvious charisma, a trait that would come in handy when conducting operations under an alias.

Svechinskaya, one of four New York University students involved in the crime, reportedly left behind a rough life in Russia. Her father had died, and her mother and grandmother lived in near poverty. Investigators say the crime was organized and planned in Eastern Europe, and eventually implemented in New York.

What investigating officers called “one of the largest cybercriminal cases” they had ever dealt with relied on a Trojan which monitored key strokes in order to steal passwords. The organization then used the passwords to siphon at least $2 million a month, according to the FBI.

The sentence was expected to be announced in June 2011, but after the arrest Svechinskaya signed a personal recognizance bond and was released under $25 thousand bail. In case of conviction, Svechinskaya could have been imprisoned for up to 40 years.

Since Svechinskaya’s release in 2013, not much new information about the notorious cyber bank robber is available. In 2016, Svechinskaya appeared in a Youtube promo for a company called Flashsafe. The company, founded by Alexander Krysin and Aleksei Churkin, builds memory-sticks with unlimited cloud storage and secure encryption to protect your personal information. A recent Facebook post showed Svechinskaya living in Brooklyn, New York and promoting a party entertainment service called Universe11.

https://www.businessinsider.com/kristina-svechinskaya-verdict-in-spring-2013-
https://alchetron.com/Kristina-Svechinskaya
https://www.technotification.com/2016/06/female-hackers-in-the-world.html
https://techframework.com/kristina-svechinskaya-worlds-most-notorious-cyber-bank-robber/

Exercise 120

Answer the questions on the text:

1. What are the most common stereotypes about hackers?
2. What malware did Kristina Svechinskaya use?
3. Was she arrested?
4. Is there any information about her present life?

SPEAKING

Exercise 121

The class is divided into 2 groups. Group A stands for white-hat hackers, Group B stands for black-hat hackers. First, discuss with your groupmates the advantages and disadvantages of your role model. Then be ready to present your ideas to the opposite group. The goal is to make a student from the opposite group to "change his hat". Groups should take turns.

LISTENING II

Exercise 122

Have you ever written a CV?

a. Watch a video "Writing a CV for students without experience" at https://www.youtube.com/watch?v=aArb68OBFPg

b. WHILE YOU WATCH. Complete the table with the information from the video:

STEP	IMPORTANT NOTES
1.	
2.	
3.	
4.	

5.	
6.	
7.	
8.	

c. AFTER YOU WATCH. Study this CV model and use it in your CV:

Name Surname
name.surname@gmail.com Phone number
8 Street Name, City, Country Social network links

PROFILE

A [your degree name] student at the [your university name] with [your best achievements and work experience]. Possess [your technical skills, your language skills and your soft skills]. Keen to pursue a career in [sector name and type of roles].

EDUCATION

University Name | City, Country ***Mmm YYYY – Mmm YYYY***
Name and Type of Degree
Predicted Grade: Grade Level
Key Modules: Key Modules Names
Dissertation / Diploma Project: 'Name of Dissertation'
Award: Name of the Award

High School Name | City, Country ***Mmm YYYY – Mmm YYYY***
High School Qualification Name *Mmm YYYY – Mmm YYYY*
Subjects: Subject Name (Grade), Subject Name (Grade), Subject Name (Grade)
Secondary School Qualification Name *Mmm YYYY – Mmm YYYY*
Subjects: Subject Name (Grade), Subject Name (Grade), Subject Name (Grade)

VOLUNTEERING

Company Name | City, Country ***Mmm YYYY – Present***
Your Position

- Provide exact details of your responsibilities
- Include which skills you have acquired
- Include which results you have achieved

ACHIEVEMENTS

- Position of Responsibility at Society Name at University Name (*YYYY-YYYY*)
- Winner of '*Name of Competition'* YYYY at University Name

ADDITIONAL SKILLS

Languages: Language (*Level*), Language (*Level*), Language (*Level*)
Microsoft Office: Proficient in Word, Excel and PowerPoint
Skill: Proficient in ….

HOBBIES & INTERESTS

Hobby Name: exact details of your hobby, with achievements and results
Hobby Name: exact details of your hobby, with achievements and results
Notes:
Soft skills *- под этим термином подразумевают широкий спектр умений. Он включает умение организовывать командную работу, вести переговоры и договариваться с коллегами, креативность, способность учиться и адаптироваться к изменениям.*

WRITING

Exercise 123

Write a CV for a job of you dream. See Ex. 32 c) for the example.

TRANSLATION PRACTICE

Exercise 124.

Translate the texts into Russian:

TEXT A
A FLORIDA TEEN HACKS THE DEPARTMENT OF DEFENSE AND NASA

In 1999, a 15-year-old north Floridian penetrated into Department of Defense and NASA computers, earning himself a spot in the hacker hall of fame. Jonathan James, who operated under the internet name "c0mrade," was a pioneer in several respects. Not only was he recognized for his high-profile hack at such a tender age; he also became the first juvenile hacker sentenced to serve prison time.

The majority of James' hacking exploits occurred between late August and October of 1999, when he breached various systems including telecommunications giant Bellsouth and the Miami-Dade school system.

But what really put James on the map was his invasion of computers used by the Defense Threat Reduction Agency (DTRA), a division of the U.S. Department of Defense tasked with monitoring threats from nuclear, biological, chemical, conventional and special weapons. James later told the Justice Department he installed a backdoor into a computer server in Dulles, Virginia, through which he was able to get more than 3,300 email messages from DTRA employees and at least 19 user names and passwords.

James was able to enter 13 computers at the Marshall Space Flight Center in Huntsville, Alabama. While there, he stole data and downloaded $1.7 million in NASA proprietary software used to support the International Space Station's physical environment, including control of the temperature and humidity within the living quarters.

After the illegal entry was discovered, NASA was forced to shut down their computers for three weeks to check and repair the system at an estimated cost of $41,000.

Agents from the Department of Defense and NASA, in conjunction with local authorities, raided James' house on Jan. 26, 2000, and he was ultimately sentenced to seven months of house arrest and probation until he turned 18. But when James violated his probation by testing positive for drugs, he was taken into custody by the U.S Marshals Service and served six months at a federal correctional facility in Alabama.

Because he was a juvenile defendant, James likely would have remained anonymous, but his father, Robert, a computer-systems analyst, released his son's name (with a hint of pride) after he pleaded guilty. Discussing his arrest with "Frontline," James said he could have easily gotten away with his crimes if he had bothered to cover his tracks, but he took no measures to hide himself because he didn't

think he was doing anything wrong. He said he was just "playing around" and didn't do anything to harm Department of Defense and NASA systems. As for lessons learned:

"I certainly learned that there's a serious lack of computer security," James told "Frontline." "If there's a will, there's a way, and if a computer enthusiast such as myself was determined to get into anywhere, be it the Pentagon or Microsoft, it's been demonstrated that it's possible and they will do it. And there's next to nothing they can do about it, because there's people with skill out there, and they'll get what they want."

James' story came to a sad end in 2008, when he committed suicide after being accused of conspiring with other hackers to steal massive amounts of personal and credit card information from department store chain TJX and other prominent retailers. While he believed he would be prosecuted for this crime, he denied any involvement.

https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-a-florida-teen-hacks-the-department-of-defense-and-nasa/

TEXT B*

WHAT IS A CYBERCRIME INVESTIGATION?

A comparison of cybercrime investigations and physical-world criminal investigations shows a difference: evidence in criminal investigations is mostly digital in nature.

A cybercrime investigation is the process of investigating, analyzing, and recovering data for digital evidence of a crime. Examples of evidence in a cybercrime investigation include a computer, cellphone, automobile navigation system, video game console, or other networked device found at the scene of a crime. This evidence helps cybercrime investigators determine the perpetrators of a cybercrime and their intent.

Cybercrime investigators perform many tasks, including determining the nature of a cybercrime, conducting an initial investigation, identifying possible digital evidence, performing digital forensics on devices, securing digital devices and evidence, and presenting evidence in the judicial system.

The criminal justice system is made up of a network of agencies, including law enforcement, the judiciary, and corrections. Individuals who work in criminal justice agencies include law enforcement officers, prosecutors, and judges. These agencies work independently, yet work together to investigate and prosecute violations of cybercrime laws. Each branch of the criminal justice system is responsible for a certain area of the criminal justice process.

Law enforcement (police officers, agents, and investigators) is responsible for gathering evidence of a crime, arresting a suspect, and charging the suspect with the crime. The judiciary consists of lawyers who present their evidence against the charged individual, lawyers who defend the individual, judges who preside over the proceedings, and juries who decide whether the individual is guilty or innocent. Corrections agencies ensure that prosecuted criminals remain behind bars during their sentences.

The FBI is the primary federal law enforcement agency that investigates cybercrime domestically and abroad. Other agencies include the U.S Secret Service, U.S. Immigration and Customs Enforcement (ICE), U.S. Postal Inspection Service, and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF). These agencies have local offices in each state. State and local law enforcement agencies also investigate cybercrimes that take place in their jurisdictions.

The private sector remains one of the most vulnerable to internal and external threats. Many of the largest companies have their own cybersecurity departments to monitor and prevent cyberattacks. Some private sector companies hire specialized cybersecurity firms to help them defend against cyberattacks.

Activities that a computer crime investigator performs include recovering file systems of hacked computers, acquiring data that can be used as evidence to prosecute crimes, writing reports for use in legal proceedings, and testifying in court hearings. Cybercrime investigation techniques include:

Performing background checks: Establishing the when, where, and who of a crime sets the stage for an investigation. This technique uses public and private records and databases to find out the backgrounds of individuals potentially involved in a crime.

Gathering information: This technique is one of the most critical in cybercrime investigations. Here, investigators ask questions such as: What evidence can be found? What level of access to sources do we have to gather the evidence? The answers to these and other questions provide the foundation for a successful investigation.

Running digital forensics: Cybercrime investigators use their digital and technology skills to conduct forensics, which involves the use of technology and scientific methods to collect, preserve, and analyze evidence throughout an investigation. Forensic data can be used to support evidence or confirm a suspect's involvement in a crime.

Tracking the authors of a cybercrime: With information about a crime in hand, cybercrime investigators work with internet service providers and telecommunications and network companies to see which websites and protocols were used in the crime. This technique is also useful for monitoring future activities through digital

surveillance. Investigators must seek permission to conduct these types of activities through court orders.

https://online.maryville.edu/blog/cyber-crime-investigation/

LISTENING III

Exercise 125

You are going to watch a video "What is cryptojacking?" at https://www.youtube.com/watch?v=Nez-niwd63Y

a. BEFORE YOU WATCH. Answer the questions:

1. Have you ever heard of cryptojacking?
2. Who may be the victim of it?

b. WHILE YOU WATCH. Fill in the gaps:

Cryptojacking! It sounds like the title of a high-tech crime movie, but cryptojacking isn't 1) _____. It's fact. And whether or not you use cryptocurrency you are at risk of becoming a 2) _____ of cryptojacking. Let's set the scene.

Crypto is 3) _____ or 4) _____ currency. It operates through a distributed database called 5) a _____. Recent transactions are combined into blocks. Blockchains are regularly updated with information about these transactions. Producing new blocks requires a lot of 6) _____ power.

Cryptocurrency companies trade cryptocurrency with people who supply the necessary computing power. They are called 7) _____. Larger cryptocurrencies use teams of 8) _____ running dedicated mining 9) _____. This activity requires a significant amount of 10) _____. Because of the huge costs of mining hardware and electric bills a new form of 11) _____ has arisen – cryptojacking.

Cryptojacking allows 12) _____ to mine for cryptocurrency without the need for extra computing or a high electric bill. That's because it's done on a 13) _____ or 14) _____ without their knowledge.

c. AFTER YOU WATCH. Answer the questions:

1. How do hackers gain access to a victim's electronic device?

2. Does crypto mining harm the victim’s device?
3. How can you tell if you are the victim of cryptojacking?
4. What can you do about it?

TEST 4.
PEOPLE IN CYBERCRIME

Choose the correct word(s) to complete the sentences:

1. A person who searches and prosecutes cybercriminals is a…
a) jury;
b) white-hat hacker;
c) cybercrime investigator;
d) law enforcement agency.

2. Any …'s standard request is not a sufficient basis for us to disclose any information.
a) police;
b) cybercrime investigator;
c) hacker;
d) law enforcement agency.

3. An ethical security hacker is a…
a) cybercrime investigator;
b) black-hat hacker;
c) white-hat hacker;
d) malefactor.

4. A person who has suffered the effects of cybercrime is called a (an)…
a) intruder;
b) malefactor;
c) victim;
d) fraud.

5. Unfortunately, my twitter account was … in the last days.
a) hacked;
b) hacking;
c) broken;
d) damaged.

6. This … made me … a lot of money.
a) malware, to pay;

b) ransomware, pay;
c) ransomware, to pay;
d) malware, paying.

7. We consider this malware …
a) to have been designed a few months ago;
b) being designed a few months ago;
c) has been designed a few months ago;
d) was designed a few months ago.

8. His employer wants him …
a) refreshing cybersecurity software;
b) refresh cybersecurity software;
c) refreshed cybersecurity software;
d) to refresh cybersecurity software.

9. The investigator made this cybercrime gang …
a) confessing;
b) confess;
c) to confess;
d) be confessed.

10. I wouldn't like my backups …
a) be stolen;
b) to be stolen;
c) stealing;
d) steal.

11. The police saw him …
a) entering the train;
b) to enter the train;
c) to have entered the train;
d) entered the train.

12. We heard him …
a) has been arrested;
b) will be arrested;

c) be arrested;
d) is arrested.

13. A person who steals money through the Internet is usually called a…
a) cyberfraud;
b) cyber stalker;
c) white-hat hacke;
d) benefactor.

14. The investigators noticed him …
a) hacked NASA cybersecurity system;
b) to hack NASA cybersecurity system;
c) was hacking NASA cybersecurity system;
d) hack NASA cybersecurity system.

15. Kevin Mitnick is considered to …
a) be a white-hat hacker;
b) be a black-hat hacker;
c) be a cybercrime investigator;
d) wear both hats.

Unit 5. Cybercrime Prevention

LEAD IN

Work in pairs and explain what we usually mean by this saying. Who can use that and in which situation?

"An ounce of prevention is worth a pound of cure"

Do you agree with the statement below? Explain your opinion:

"If you think you know it all about cybersecurity, this discipline was probably ill-explained to you"

by Stephane Nappo

KEY TERMS

a cyber incident	кибератака
an accidental action	непреднамеренное действие
a deliberate action	умышленное действие
a third party	*юр.* сторонняя организация
to compromise (a target)	взломать, рассекретить зашифрованные материалы
threat environment	угрожающая среда
regulatory tools	нормативно-правовые инструменты
to tackle (cybercrime)	предотвращать
deterrence	сдерживание
to foster (cooperation)	поощрять, поддерживать
capacity (in Law)	*юр*. дееспособность, правоспособность
cyber-enabled, cyber-dependent (crimes)	возможные благодаря киберпространству или пользующиеся киберпространством
forensic standards	стандарты расследования
sexual abuse	сексуализированное насилие
stakeholder	вовлеченная сторона
darknet	даркнет, «темный Интернет»
digital footprints	цифровой след

to jeopardize	подвергать риску
credentials	учетные данные
cybersecurity assessment	тест кибербезопасности
penetration testing	тестирование на проникновение
red teaming	имитация реальной атаки
reconnaissance	рекогносцировка
leaked (data)	слитый (о данных)
phishing	фишинг, обман с целью получения доступа к учетным данным
smishing	смишинг, фишинг через СМС
credential stuffing	подстановка учетных данных
brute-force attack	атака полным перебором

Exercise 126

a. What parts of speech are the following words?

Accident, accidental, compromise, forensic, forensics, deter, deterrence, assess, access, assessment, jeopardize, jeopardy, regulate, regular, regulatory, stuff, stuffing.

b. Identify roots, stems, suffixes and translate the words.

Exercise 127

Which word is odd?

accidental	intentional	deliberate	voluntary
compromise	hack	tackle	penetrate
jeopardize	violate	protect	abuse
stakeholder	participant	main party	third party
darknet	deepnet	clearnet	hidden Internet
secure	leaked	exposed	compromised
phishing	smishing	red teaming	credential stuffing

Exercise 128

a. Match the words with similar meaning:

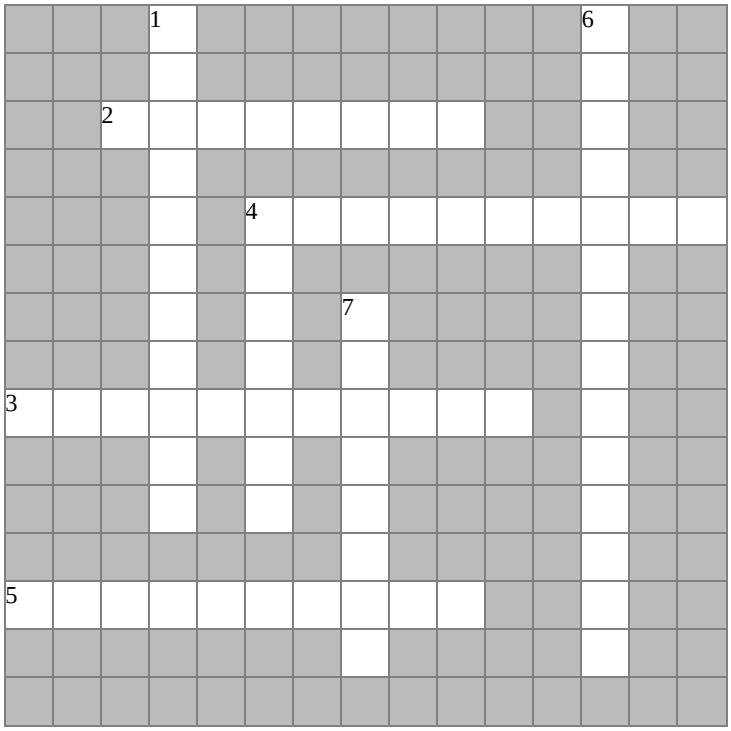
1) to foster	a) liability
2) to jeopardize	b) survey
3) deterrence	c) to nurture
4) reconnaissance	d) cyber-enabled
5) cyber-dependent	e) to risk
6) capacity	f) passwords
7) credentials	g) defense

b. Match the words with opposite meaning:

1) stakeholder	a) deliberate
2) to tackle	b) safe
3) leaked	c) cyber incident
4) darknet	d) to support
5) accidental	e) safe environment
6) threat environment	f) clearnet
7) penetration testing	g) a third party

Exercise 129

Solve the puzzle:



Horizontally:

2. a quality denoting the legal aptitude of a person to have rights and liabilities
3. login details, cryptographic keys, passwords which are used to establish the identity of a user
4. operations undertaken to prevent cybercriminals from initiating any aggressive actions
5. the information about a particular person that exists on the internet as a result of their online activity is called "digital …"

Vertically:

1. a person, group or organization with a vested interest in the decision-making
4. a computer network that uses the internet but can only be joined by people who have permission or who have the right software
6. preliminary surveying or research, the information-gathering stage of ethical hacking
7. a form of social engineering where attackers deceive people into revealing sensitive information, e.g. login credentials and credit card numbers

Exercise 130

Match the word combinations:

1) threat	a) stuffing
2) credential	b) testing
3) a deliberate	c) a cybercrime
4) to tackle	d) environment
5) penetration	e) standards
6) forensic	f) cooperation
7) to foster	g) action

Exercise 131

Complete the following sentences using the words and word combinations from the previous tasks (the first letter is given in brackets):

1. The Committee worked on legislation properly and introduced new r_____ t_____ that would help to t_____ cybercrime more effectively.

2. L_____ passwords were sold in d_____, so criminals could access sensitive information using c_____ s_____.
3. We paid for the service to a t_____ p_____, an independent cybersecurity agency, and that was the best solution. They run all kinds of c_____ a_____ including p_____ t_____.
4. R_____ t_____ highlighted several serious weaknesses that could potentially j_____ our clients' bank accounts.
5. The Criminal Code defined strict f_____ s_____ to counter child s_____ a_____ and prosecute criminals who left their d_____ f_____ on websites containing such videos.
6. "The Dark Overlord" gang created a database of compromised c_____.
7. R_____ is the first step that is involved in the process of ethically hacking or penetrating a cyber asset.
8. These hackers initiated b_____ a_____ generating as many passwords as they could.

Exercise 132

Translate these sentences from Russian into English using the words and word combinations from the previous tasks:

1) Непреднамеренная ошибка одного из топ-менеджеров создала серьезную угрозу кибербезопасности этой большой корпорации.
2) И вовлеченные стороны, и сторонние организации должны понимать, что находятся в угрожающей среде.
3) Рекогносцировка показала, что два года назад была предпринята атака полным перебором.
4) Имитация реальной атаки недавно подтвердила способность фирмы предотвращать киберугрозы.
5) Ваши учетные данные были рассекречены. Теперь каждый может найти эти слитые пароли в даркнете.
6) Цифровые следы навели следователей на банду, которая с помощью фишинга в социальных сетях для знакомств завладела данными банковских карт многих пользователей.
7) Случаи сексуализированного насилия в Интернете до сих пор нуждаются в более надежных регуляторно-правовых инструментах и новых стандартах расследований.

8) Никто не может гарантировать, что тестирование на проникновение не нарушит работу рабочей почты в течение дня.
9) Смишинг в ближайшем будущем будет более распространен, чем фишинг, считает наш специалист по кибербезопасности.
10) Ваши умышленные действия подвергли риску персональные данные всех сотрудников. Теперь кто угодно может зайти на главный сайт, воспользовавшись простой подстановкой данных.

Exercise 133

Work in pairs. Discuss the questions:

1. What laws are needed to protect cybersecurity?
2. How has the situation with cybercrimes changed in recent years?
3. What legal bodies may help national states to combat cybercrime?
4. What strategic initiatives would be important for cybersecurity?

READING I

Exercise 134

Read the excerpt from The EU's Cybersecurity Strategy for the Digital Decade. Name several tools which the EU Commission uses for cybercrime prevention.

THE EU'S CYBERSECURITY STRATEGY FOR THE DIGITAL DECADE (EXCERPT)

Cyber incidents, whether accidental or the deliberate action of criminals, state and other non-state actors, can cause enormous damage. Their scale and complexity, often involving the exploitation of third-party services, hardware, and software to compromise a final target, make the EU’s collective threat environment hard to counter without systematic and comprehensive information sharing and cooperation on a common response. The EU aims, through the full implementation of regulatory tools, mobilisation and cooperation, to support Member States in defending their citizens, as well as their economic and national

security interests, in full respect of fundamental rights and freedoms and the rule of law.

Our dependence on online tools has exponentially increased the attack surface for cyber criminals, and led to a situation where the investigation of nearly all types of crime has a digital component. Furthermore, core parts of our society are threatened by cyber actors and by those using cyber tools to plan and execute their illegal actions.

Tackling cybercrime effectively is a key factor in ensuring cybersecurity: deterrence cannot be achieved through resilience alone but also requires identification and prosecution of offenders. It is therefore essential to foster the cooperation and exchange between cybersecurity actors and law enforcement.

As one important element of that response, EU and national authorities need to expand and improve the capacity of law enforcement to investigate cybercrime, fully respecting fundamental rights and pursuing the required balance between various rights and interests. The EU should be able to tackle cybercrime through fully implemented legislation that is fit-for-purpose, with a particular focus on digital investigations, including criminality on the 'darknet'. Law enforcement must be fully equipped for digital investigations. The Commission will therefore put forward an action plan to improve digital capacity for law enforcement agencies, by providing them with the necessary skills and tools. In addition, Europol will further develop its role as a centre of expertise to support national law enforcement authorities combatting cyber-enabled and cyber-dependent crime, contributing to the definition of common forensic standards.

Strategic initiatives

The EU should:

- Define a set of objectives in international standardisation processes, and promote these at international level;
- Advance international security and stability in cyberspace, notably through the proposal by the EU and its Member States for a Programme of Action to Advance Responsible State Behaviour in Cyberspace (PoA) in the United Nations;
- Offer practical guidance on the application of human rights and fundamental freedoms in cyberspace;
- Better protect children against child sexual abuse and exploitation, as well as a Strategy on the Rights of the Child;
- Strengthen and promote the Budapest Convention on Cybercrime, including through the work on the Second Additional Protocol to the Budapest Convention;

- Expand EU cyber dialogue with third countries, regional and international organisations, including through an informal EU Cyber Diplomacy Network;
- Reinforce the exchanges with the multi-stakeholder community, notably by regular and structured exchanges with the private sector, academia and civil society.

https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade

Exercise 135

Decide if the statements are true or false. Correct the false statements.

STATEMENT	**TRUE**	**FALSE**
1. Accidental cyber incidents cannot cause a lot of damage		
2. The scale of cyber incidents makes it hard to counter without systematic cooperation.		
3. The EU aims to support Member States in offending their citizens without any respect of fundamental rights and freedoms.		
4. Our dependence on online tools has exponentially decreased the attack surface for cyber criminals.		
5. The investigation of nearly half of types of crime has a digital component		
6. Deterrence cannot be achieved through resilience alone		
7. EU and national authorities need to reduce the capacity of law enforcement.		
8. The EU should be offered practical guidance on the application of human rights and fundamental freedoms in cyberspace.		
9. The EU should reinforce the exchanges the private sector, academia and civil society.		

Exercise 136

Find in the text words with hyphen (-). Can you say what they mean without looking at the dictionary?

Exercise 137

Find Modal verbs and their equivalents used in the text. What modality (possibility, obligation, etc.) most of them express and why?

Exercise 138

Restore the words in the following sentences:

1. Cyber incidents, whether accidental or the ***eableiertd*** action of criminals, state and other non-state actors, can cause enormous damage.
2. Cybercrimes often involve the exploitation of third-party services, hardware, and software to ***opiomrsemc*** a final target.
3. Furthermore, core parts of our society are ***enehaetrtd*** by cyber actors and by those using cyber tools to plan and execute their illegal actions.
4. It is therefore essential to ***eosftr*** the cooperation and exchange between cybersecurity actors and law enforcement.
5. The EU should be able to ***celatk*** cybercrime through fully implemented legislation.
6. Europol will further develop its role as a centre of ***rtpsiexee*** to support national law enforcement authorities/
7. The EU should advance international security and stability in ***ecraesypcb***.
8. The EU should ***nsghtreent*** and promote the Budapest Convention on Cybercrime.

Exercise 139

a. Look through the excerpt about the EU Joint Cyber Unit and complete its description with the words and word combinations from the box:

response large-scale recovery virtual preparedness incidents and threats stakeholders facilitate objectives focus assistance

A Joint Cyber Unit

A Joint Cyber Unit would serve as a _____ and physical platform for cooperation for the different cybersecurity communities in the EU, with a _____ on operational and technical coordination against major cross-border cyber _____.

This could address two main gaps that currently increase vulnerabilities and create inefficiencies in the _____ to cross-border threats and incidents affecting the Union. Firstly, civilian, diplomatic, law enforcement and defence cybersecurity

communities do not yet have a common space to nurture structured cooperation and _____ operational and technical cooperation. Secondly, relevant cybersecurity _____ have not yet been able to tap into the full potential of operational cooperation and mutual _____ within existing networks and communities. The Unit should improve and accelerate coordination and allow the EU to face up and respond to _____ cyber incidents and crises.

The Joint Cyber Unit would fulfil three main _____. Firstly, it would ensure _____ across cybersecurity communities; secondly, through information sharing it would provide continuous shared situational awareness; thirdly, it would reinforce coordinated response and _____.

Exercise 140

Read the fragments and find their beginnings in the left column.

1. EU rules on the security of Network and Information Systems (NIS) are at the core of the Single Market for cybersecurity.	a. This is because national authorities do not systematically gather and share information - such as that available from the private sector - which could help assess the state of cybersecurity in the EU. Only a fraction of incidents are reported by Member States, and information sharing is neither systematic nor comprehensive.
2. The EU's critical infrastructure and essential services are increasingly interdependent and digitised.	b. Over two-thirds of companies are considered 'novices' in cybersecurity, and European companies are considered less well prepared than companies in Asia and America. An estimated 291 000 posts for cybersecurity professionals in Europe remain unfilled. Hiring and training cybersecurity experts is a slow process leading to greater cybersecurity risks for organisations.
3. A set of core protocols and supporting infrastructure ensures the functionality and	c. The Commission proposes to reform these rules under a revised NIS Directive to increase the level of cyber resilience of all relevant sectors, public and private, that perform an important function for the economy and society. The review is necessary to reduce inconsistencies across the internal market by aligning scope, security and incident reporting

integrity of the Internet worldwide	requirements, national supervision and enforcement and the capabilities of competent authorities.
4. There is a major shortage of cybersecurity skills in the workforce	d. This set includes the DNS (Domain Name System) and its hierarchical and delegated system of zones, starting, at the top of the hierarchy, with the root zone and the thirteen DNS root servers on which the World Wide Web depends. The Commission intends to develop a contingency plan, supported by EU funding, for dealing with extreme scenarios affecting the integrity and availability of the global DNS root system.
5. The EU lacks collective situational awareness of cyber threats	e. All Internet-connected things in the EU, whether automated cars, industrial control systems or home appliances, and the whole supply chains which make them available, need to be secure-by-design, resilient to cyber incidents, and quickly patched when vulnerabilities are discovered. This is fundamental to provide the EU's private and public sector with the possibility to choose from the most secure infrastructures and services.

Exercise 141

Answer the questions:

1. What does the EU lack in cybersecurity?
2. What is DNS and how many DNS root servers are there in the world?
3. What proportion of companies are considered 'novices' in cybersecurity?
4. Who wants to reform rules on the security of Network and Information Systems?
5. What requirements are imposed on all Internet-connected things in the EU?
6. How many posts for cybersecurity professionals remain unfilled?

Exercise 142

What other documents on cybercrime prevention are mentioned in the first text? Are you familiar with any of them? Translate the document titles into Russian. Discuss your variants of translation with the group and your teacher.

Правила юридического перевода

Вы уже знаете, что юридический перевод нацелен на точную передачу информации. Для этого переводчики юридических текстов пользуются речевыми клише, сокращениями, профессиональными терминами. При переводе

названий важных документов важно пользоваться устоявшимися вариантами перевода и, когда есть возможность, уточнять корректность перевода в специализированных словарях или в статьях ведущих информагентств (например, ТАСС).
Например,
The EU's Cybersecurity Strategy for the Digital Decade – Стратегия кибернетической безопасности ЕС
The Budapest Convention on Cybercrime – Будапештская конвенция по борьбе с киберпреступлениями

LISTENING I

Exercise 143

You are going to listen to the review on the book "Hunting Cyber Criminals: A Hacker's Guide to Online Intelligence Gathering Tools and Techniques" by Vinni Troia at https://youtu.be/x0tL4U22SI8 (00:00 - 4:30)
a. BEFORE YOU WATCH. Answer the questions:

1. What tools and techniques can be used in digital investigation? Have you ever heard of OSINT (open-source intelligence)?
2. What kind of mindset a digital investigator should have?
3. Is there anything what makes digital investigations similar to those in the offline world?

b. WHILE YOU WATCH. Fill in the gaps (the first letter is given):

1. The author, Vinny Troia, has tracked t____ a___ (*2 words*) across the Internet for several years now, culminating in the unmasking of one of the primary members of a cybercrime group called The Dark Overlord, that's been stealing organizations' data and selling them on the b____ m____ (*2 words*) since 2016.
2. The group later changed their tactics to terrorizing victims with all kinds of threats and e_____ them for money.
3. The book takes us through a maze of deception spanning social media, b_____ f____ (2 words), to underground cybercrime markets.
4. Rather than just a laundry list of tools, the author generously shares his arsenal of methods and the process he used to t____ d____ (2 words) targets.

5. He describes himself as a “puzzle junkie”, who’s r_____ when it comes to finding answers to complex problems, even if it means sleepless nights awake in the morning cranking away at something.
6. Unlike all the media out there discussing whether or not some coin’s value is going to the moon or all the technical wonders of distributed edger technology, the book focuses on the investigative aspects of cryptocurrencies when they’re used in economic transactions for s____ and cybercrime markets on the d_____.
7. High-fidelity threat intel comes from actively working your way into cybercrime groups as a t_____ i_____ (2 words), in order to gather more information.
8. This might bring you into gray areas, since the people you’re collaborating with usually value money over moral or legal b_____ and expect you to do the same.
9. If you’re patient and resolved, cybercrime networks slip up from time to time and reveal v_____ too.
10. Once you’ve latched on, cyber criminals will often give away the greatest clues about their i_____ simply out of fear and self-preservation.

Now you are going to watch the same review with subtitles. Take notes while listening.

c. AFTER YOU WATCH. Answer the questions:

1. How many years did Vinny spend to track down “The Dark Overlord” group? How many core members were there?
2. What methods and tools can you learn after reading the book?
3. What are the main skills for offensive and defensive cyber specialist?
4. What is important for a digital investigator about cryptocurrencies?
5. How can you get clues to identities of cyber criminals?

d. Discuss with the group possible translation of these phrases into Russian.

1. The book *takes us through a maze of deception* spanning social media, blackhat forums, to underground cybercrime markets.
2. This is so much more helpful than a lot of guides and manuals out there that don’t really focus on *the mental workflow* and the how of *getting from point A to point B* in an investigation.
3. He also *scatters gems of wisdom* from a dozen other experts like John Strand, Leslie Carhart, and Chris Hadnagy.

4. He describes himself as a *"puzzle junkie",* who's relentless when it comes to finding answers to complex problems, even if it means sleepless nights awake in the morning *cranking away at something*.
5. This attitude is key for professionals in the cybersecurity field, since a lot of the work is troubleshooting and solving problems, which usually involves seriously *grokking of how a system works*.
6. Tracing these transactions to find out which *entities* own which wallets is essential to tracking the people in *the online underground.*
7. Real investigations are dirty, since you've gotta build *a web of aliases* and deep *cover stories* for each.
8. Direct communications with threat actors can reveal valuable intelligence on their *modus operandi* and internal structures.
9. If you *don't play the game*, *you'll be discovered and outed* as an investigator. It's just like the drug gang that makes everyone involved partake in the drugs, *to try and sniff out any feds* [federal investigators].
10. If you're patient and resolved, cybercrime networks *slip up from time to time* and reveal vulnerabilities too. Once *you've latched on*, cyber criminals will often give away the greatest clues about their identities simply out of fear and self-preservation.

GRAMMAR

Exercise 144

Study grammar rules on the use of COMPLEX SUBJECT (see GRAMMAR REFERENCE pp. 178-179). Translate the sentences into Russian paying attention to the infinitive and participle structures:

1. This attitude is believed to be key for professionals in the cybersecurity field
2. These rules are supposed to be reformed.
3. The book by Vinny Troia is considered to be a full guide to cybercrime prevention.
4. He is likely to write another book on hunting cybercriminals.
5. She was noticed to be chatting with contacts from "The Dark Overlord" on blackhat forums.
6. They are heard to have revealed their identities due to calling each other real names in a secret chat.
7. Vulnerabilities were supposed to be patched.
8. The primary members of a cybercrime group are said to have been arrested.

9. This notorious hacker is unlikely to be impressed by her cover story.
10. Real investigations are believed to be dirty.

Exercise 145

Reconstruct the phrases using Complex Subject.
Example: It is supposed that he is solving the problem. – *He is supposed to be solving the problem.*
1. It is believed that transactions in cryptocurrencies are anonymous.
2. It was likely that "The Dark Overlord" will slip up eventually.
3. It is noticed that digital investigators use new regulatory tools to prevent cybercrime.
4. It is believed that the accountant is stealing money from clients using her cryptocurrency wallet.
5. It was said that a web of aliases was an urgent need.
6. It is reported that the suspect has left the country.
7. It is sure that your boss did not change the standard password.
8. It is unlikely that this firm value moral boundaries over money.
9. It is expected that red teaming will discover new vulnerabilities.
10. It is known that she tracked down these notorious hackers.

READING II

OSINT – OPEN -SOURCE INTELLIGENCE

OSINT finds digital footprints that are publicly accessible in any format, including videos, images, conferences, research papers, webinars, etc. It is recognized as a legal activity as long as the person does not break the law, jeopardizes an individual's privacy, or violates the copyrights.

In cybersecurity, OSINT helps discover compromised and breached credentials, publicly available business records, individuals or organization's personal and background information, documents, image-focused searches, email, and domain information, inter-connected devices or applications information, exploits archives, removed but indexed data, geolocation information, darknet resources, blogs, news, social media content or profiles, etc.

Just like everything comes with pros and cons, OSINT can be used in both ways. Notably, in ethical hacking, OSINT helps discover the digital footprints in various

cybersecurity assessments such as penetration testing, red teaming, social engineering, threat intelligence, etc. While utilizing the publicly available information, security professionals and organizations identify sensitive, exposed information that could allow any ill-intentioned hacker to use and launch an attack on the critical assets.

Similarly, in black-hat hacking, malicious attackers use open-source intelligence (OSINT) to retrieve information about their target in order to pick potential vulnerable or beneficial access points that could help them gain data, information or identify a roadmap to develop an attack plan.

OSINT has a significant role in identifying internal and external threats and vulnerabilities in any organization's digital environment and its assets. In information security, for most of the assessment (e.g., penetration testing, red team assessment), information gathering is the first step of security testing. This step is usually termed *reconnaissance* in the information and cybersecurity sector.

While doing the reconnaissance, the ethical hacker/security expert collects information about the target such as domain, subdomain, person, organization, and employee's sensitive information, inter-connected devices, open ports, software, public business records, the website listed directories, and other exposed assets as well as leaked information, e.g., employees' credentials, business secrets/records, etc. in any previous breaches or available over the dark web to identify the sensitive, exposed data, vulnerable access points, and security gaps to mitigate them.

For instance, in social engineering assessment, security professionals look out for employees' details such as social media and other application profiles, e.g., Trello, Dropbox, Outlook, etc., to track their activities for phishing, smishing attacks. In the same manner, exposed and compromised credentials help launch various password attacks, e.g., credential stuffing, brute-force attacks, etc., to have malicious access to systems, applications, servers, etc.

There are numerous OSINT tools, here are some of the resources that can be used to collect information:

Google – an essential element of OSINT, if you learn the art of googling, you already completed 85% of OSINT research.

Other than Google, one can use

Have I been Pwned – to look out for breached emails

Dehashed – for compromised account password

Pentest tool – for subdomain collection

DNSDumpster – for DNS records

Shodan – for internet-connected device information

https://iosentrix.com/blog/How-OSINT-is-used-in-Cybersecurity-Part-1/

Exercise 146

Decide if the statements are true or false. Correct the false statements.

STATEMENT	TRUE	FALSE
1. OSINT finds as many information about target as possible, even if it jeopardizes an individual's privacy.		
2. OSINT studies compromised and breached credentials as well as blogs, news, social media content or profiles.		
3. OSINT is used only by white-hat hackers.		
4. Information gathering, which is the second step of security testing, is termed reconnaissance.		
5. Ethical hackers never collect sensitive information.		
6. Social engineering assessment is not a usual task for a cybersecurity professional.		
7. Criminal can use exposed and compromised credentials help launch various password attacks.		
8. Google is too simple to be a tool for OSINT.		
9. Dehashed gives you access to DNS records.		

Exercise 147

Answer the questions on the text:

1. What is OSINT?
2. Who uses OSINT and for what reason?
3. How does it help in identifying attack surface?
4. What is the first step of security testing?
5. What types of data are usually collected by a cybersecurity expert?
6. What tools can OSINT use?

Exercise 148

Work in pairs. Do an OSINT research about the given person who reluctantly shares any information in media. Then tell your partner what you got to know about them using Complex Subject.

For example,

He is said to live in Moscow

It is believed that he has met with the President once.

Student A:

Edward Joseph Snowden 	Age: Nationality: Occupation: Foreign languages: Activity in the recent years: Additional details:

Student B:

Viktor Olegovitch Pelevin 	Age: Nationality: Occupation: Foreign languages: Activity in the recent years: Additional details:

Exercise 149

Work in pairs. Read a scenario for your partner and wait for their answer. Ask them to explain their answer in terms of cybersecurity. If the given answer is not right, correct them and read the explanation. Then change roles. Don't look at the scenarios and answers of your partner!

Student A

Scenario 1

Your supervisor is very busy and asks you to log into the corporate server using her user-ID and password to retrieve some reports. What should you do?

A: It's your boss, so it's okay to do this.

B: Ignore the request and hope she forgets.
C: Decline the request and remind your supervisor that it is potentially harmful for cybersecurity.
Answer 1:
C - Decline the request and remind your supervisor that it is potentially harmful for cybersecurity.
User-ID's and passwords must not be shared. If you are pressured further, report the situation to a cybersecurity specialist.
Scenario 2
You receive an email from your bank telling you there is a problem with your account. The email provides instructions and a link so you can log in to your account and fix the problem. What should you do?
Answer 2
Delete the email. Better yet, use the web client (e.g. gmail, yahoo mail, etc.) and report it as spam or phishing, then delete it.
Any unsolicited email or phone call asking you to enter your account information, disclose your password, financial account information, social security number, or other personal or private information is suspicious – even if it appears to be from a company you are familiar with. Always contact the sender using a method you know is legitimate to verify that the message is from them.
Scenario 3
Your group mate used her Telegram account at a computer lab on campus. She made sure her account was no longer open in the browser window before leaving the lab. Someone came in behind her and used the same browser to re-access her account. They started sending spam from it and caused all sorts of mayhem in public chats.
What do you think might be going on here?
Answer 3
The first person probably didn't log out of her account, so the new person could just go to history and access her account.
Another possibility is that she did log out, but didn't clear her web cache. (This is done through the browser menu to clear pages that the browser has saved for future use.)

Student B
Scenario 1
The mouse on your computer screen starts to move around on its own and click on things on your desktop. What do you do? (There are several right actions)
A: Call your co-workers over so they can see.

B: Disconnect your computer from the network.
C: Unplug your mouse.
D: Tell your supervisor.
E: Turn your computer off.
F: Run anti-virus.
G: All of the above.
Answer 1
B & D.
This is definitely suspicious. It seems possible that someone is controlling the computer remotely, it is best if you can disconnect the computer from the network (and turn off wireless if you have it) until help arrives. If possible, don't turn off the computer.
Scenario 2
A friend sends an electronic greeting card (e-card) with a cute kitten to your work email. He wants to congratulate you with your newly acquired position in this respected company. You need to click on the attachment to see the card.
What should you do?
Answer 2
Delete the message. Some attachments contain viruses or other malicious programs, so just in general, it's risky to open unknown or unsolicited attachments. Also, in some cases just clicking on a malicious link can infect a computer, so unless you are sure a link is safe, don't click on it. Email addresses can be faked, so just because the email says it is from someone you know, you can't be certain of this without checking with the person. Finally, some websites and links look legitimate, but they're really hoaxes designed to steal your information.
Scenario 3
One of the staff members in your university subscribes to a number of free I.T. magazines. Among the questions she was asked in order to activate her subscriptions, one magazine asked for her date of birth, a second asked for the name of her hometown, and a third asked for her mother's maiden name.
What do you think might be going on here?
Answer 3
All three newsletters probably have the same parent company or are distributed through the same service. The parent company or service can combine individual pieces of seemingly-harmless information and use or sell it for identity theft.
Note: Often questions about personal information are optional. In addition to being suspicious about situations like the one described here, never provide personal

information when it is not legitimately necessary, or to people or companies you don't personally know.

SPEAKING

Exercise 150

Project Work. Read recommendations on how to prepare a project.

1) ***Preparation***. Get started on a project by discussing things in a group and plotting your research. Make a list of tasks and allocate them to each member of your group.
2) ***Research.*** Make a project outline. Use reliable and up-to-date sources. Add the information found to the shared draft of a document.
3) ***Presentation.*** Assign roles in your group: who will give a speech, who will be changing slides, who will be giving handouts to the audience… Prepare charts and graphs to illustrate your ideas.

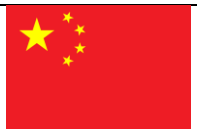
Exercise 151

a) Now you will be divided into three teams working on individual projects. You are a group of experts, and your task is to prepare new regulatory tools for bilateral cooperation against cybercrimes. First, you need to gather the data. Conduct additional research if you need more information about these countries.

Team 1

 **The United States of America**	 **Mexico**
Advantages: • Technical intelligence capabilities • Huge experience in offensive and defensive cyber operations • …	**Advantages:** • Low-cost STEM workforce • Investments to IT sector • …
Disadvantages: • Expensive workforce • Outdated standards in cybersecurity • …	**Disadvantages:** • Weak regulation of cybercrime • Low digital literacy • …

Team 2

 **Russia**	 **China**
Advantages: • Technical intelligence capabilities • Experience in offensive and defensive cyber operations • …	**Advantages:** • Investments to IT sector • Successful international IT corporations • …
Disadvantages: • Sanctions imposed on different international web services • Partial Internet censorship • …	**Disadvantages:** • The Great Firewall • Lack of experience in cyber operations • …

Team 3

 **India**	 **The United Arab Emirates**
Advantages: • A lot of English-speaking IT specialists • Investments to IT sector • …	**Advantages:** • Policies to promote the use of open data • Rapid growth in the cybersecurity market • …
Disadvantages: • Staff turnover • Weak regulation of cybercrime • …	**Disadvantages:** • Lack of specialists • Lack of experience in cyber operations • …

b) Write a document to establish or foster cooperation between two countries. Emphasize possible ways two countries may use to benefit from synergies of their advantages and counteract disadvantages.

c) Present your project to the group. You may use visual devices (graphs, charts, pictures) to illustrate your report.

LISTENING II

Exercise 152

You are going to listen to the second part of the review on the book "Hunting Cyber Criminals: A Hacker's Guide to Online Intelligence Gathering Tools and Techniques" by Vinni Troia at https://youtu.be/x0tL4U22SI8 (4:30 - 8:10)

a. BEFORE YOU WATCH. Answer the questions:

1. What is OPSEC? Find the answer on the Internet if you have never seen this abbreviation before.
2. What psychological traits of cybercriminals may jeopardize their anonymity?
3. What should the society do with young aspiring hackers to prevent them from involving in cybercrime?

b. WHILE YOU WATCH. Fill in the gaps (the first letter is given):

1. The first and foremost is that v____ always trumps OPSEC. Cyber folks spend a huge amount of time learning and perfecting their c_____.
2. Young aspiring hackers engaging in cybercrime may find it more difficult to avoid b_____ about their exploits online and might be more willing to v_____ their activities to journalists.
3. The nature of the Internet is that identifiers like domain names or IP addresses inevitably change overtime, so researching current data is guaranteed to miss c____, especially if your cybercrime target is actively cleaning up their past and hiding their tracks with d_____.
4. When you do stumble across something like a private picture or message, it's always important to keep m_____ documentation for future referencing,
5. The third theme is to never rely on a single technique to obtain answers. You might get lucky with even o_____ tools that have never produced good results.

6. Anything from a recycled profile icon or username can be a valuable piece of the puzzle in an investigation, so you want to exhaust everything at your d_____ to draw out more intel.
7. Building a meaningful operation requires e_____ a team of people to work with you, which requires trust.
8. Jealousy, betrayal, and feuds happen among blackhat circles too, which often leads to their d_____.
9. Oftentimes, it's the blackhat communities that are their g_____ into this field, which always creates opportunities for going to the dark side and getting involved in more serious cybercrime activity.
10. Mentorship, both formal and informal, can help s_____ people in the right direction towards creative productivity rather than creative thievery and destruction.

Now you are going to watch the same review with subtitles. Take notes while listening.

c. AFTER YOU WATCH. Answer the questions:

1. What desire may be a serious trouble for OPSEC? Which category of hackers is more inclined to show it?
2. Why do investigators need access to historical data? How do they get it?
3. How many techniques do professionals use for tracing cyber criminals?
4. Why does cybercrime pay well only for a short period of time?
5. Does the book contain any advice for young aspiring hackers?

d. Discuss with the group possible translation of these phrases into Russian.

1. It's hard not to like attention and recognition for your work, whether you're *a script kiddie*, or *a time-seasoned professional*.
2. Cybercrime pays well; very well actually, but only for a short period of time, since it's really hard *to execute your online personas flawlessly and compartmentalize everything*.
3. Trust is most vulnerable when *stakes and emotions run high*.
4. I certainly *got started out on the wrong foot* in the hacking scene, a long long time ago, before eventually *making my way to the light side*.
5. While it *raises the bar* to be a cyber criminal, it also *raises the bar* for investigators too, as people adapt to their tradecraft accordingly.
6. It's *the cat and mouse game* we'll never see an end to.

WRITING

Exercise 153

Have you ever written an essay?

a. Watch a video "Basic essay writing structure" at https://www.youtube.com/watch?v=zHmdOeQbjHA

b. WHILE YOU WATCH. Complete the table with the information from the video:

SECTION	FUNCTION
1.	
2.	
3.	

c. Study the linking words and use them in your essay:

To introduce topic	Firstly, … Currently/ presently… To begin with… There are differing opinions as to why
To list points	In the first place, … First of all, … To start with, … Secondly (thirdly), … Finally, … Last but not least, …
To make contrasting points	On the other hand, … However, … In spite of … While… Despite the fact that… Although… It can be argued that…

To give examples	For example, … For instance, … Or let us take another example. To take yet another illustration… Like/ especially/ such as/ in particular
To make a conclusion	Finally, …. In general, however… In short, … It seems clear that… To put it simply, … To sum it all up, …

Exercise 154

"Trust is most vulnerable when stakes and emotions run high"

Write an essay about trust in cybersecurity and cybercrime. The recommended volume is 200–250 words.

TRANSLATION PRACTICE

Exercise 155

Translate the text into Russian.

SANS INCIDENT RESPONSE FRAMEWORK

The term Incident Response refers to the processes and policies an organization utilises in response to a cyber incident such as an attack or data breach. The goal of Incident Response is to mitigate the damage of an attack i.e. reduce the recovery time, effort, costs and reputational damage associated with a cyber-attack or data breach. Apart from mitigating various consequences of a cyber attack, the process of Incident Response can help organizations prevent future attacks that threaten their information security.

The SANS Institute is a private U.S. for-profit company founded in 1989 that specializes in information security, cybersecurity training, and selling certificates. One of the main contributions the SANS Institute has made to cybersecurity is their Incident Response Framework, which has also garnered praise from organizations around the world for its comprehensiveness. The SANS Institute published a 20-page handbook that lays out a structured 6-step plan for incident response. Below is a brief summary of the process.

The SANS Incident Response Process consists of five steps:

#1 Preparation

This involves organizations performing reviews over their security policy, which typically involves risk assessments to identify vulnerabilities, sensitive assets and areas of focus in terms of security incidents. In this stage organizations also work towards forming a Computer Security Incident Response Team or CSIRT in short.

#2 Identification

In this stage, security teams monitor systems and networks to identify any suspicious activity taking place during day to day operations, in the hopes of discovering any premature security incidents. If an incident is to be discovered, security teams should document everything, e.g. the nature of the attack or it's origin.

#3 Containment

If an Incident is identified the next step that follows is containment, security teams need to work towards isolating the attack and preventing it from spreading. This can involve segmenting a network under attack as part of short term containment. Once short term measures are in place, security teams can focus on long term solutions or fixes which may involve rebuilding entire systems.

#4 Recovery

This step involves bringing back affected systems that were taken down over the period of the incident. Security teams should test and monitor affected systems to ensure that attacks don't repeat and that normal functionality is achieved.

#5 Lessons Learned

Shortly after the attack, teams need to look back and evaluate how the incident was handled and analyse how the incident response process can be improved for future incidents.

After Sam Newton "Understanding Incident Response Frameworks - NIST & SANS".
https://www.stickmancyber.com/cybersecurity-blog/incident-response-frameworks-nist-sans

TEST 5.
CYBERCRIME PREVENTION

Choose the correct variant:

1. Somebody who is involved with an organization, society, etc. and therefore has responsibilities towards it and an interest in its success is called a …
a) a third party;
b) a hacker;
c) a stakeholder;
d) a successor.

2. … is the collection and analysis of data gathered from open sources (covert and publicly available sources) to produce actionable intelligence
a) OSINT;
b) social engineering;
c) red teaming;
d) threat intelligence.

3. Among threats to children related to the e-environment, multiple forms of child … , including cyberbullying, sextortion, cyberstalking.
a) labor;
b) protection;
c) welfare;
d) abuse.

4. "… …" (sometimes 'shadow') is the body of data that an individual creates through their actions online.
a) digital investigators;
b) digital clock;
c) digital footprints;
d) digital signal.

5. This virus could … the whole national banking system.
a) jeopardize;
b) hack;
c) deter;

d) compartmentalize.

6. “Neo”, a notorious hacker, and Thomas Anderson, an insignificant clerk, … the same person.
a) are said to be;
b) is said being;
c) are said being;
d) is said to be.

7. John Snowden … in Moscow.
a) is believed to live;
b) is believed live;
c) is believe to live;
d) be believe to live.

8. Vinny Troia is reported … “The Dark Overlord” group.
a) to track down;
b) to have tracked down;
c) to be tracking down;
d) to be tracked down.

9. Look! They are likely … company’s main server with credential stuffing right now.
a) to be attacking;
b) to be attacked;
c) to have been attacked;
d) to have attacked.

10. This craft is said … from generation to generation.
a) to be passing on;
b) to be passed on;
c) to pass on;
d) to have passed.

11. One who can’t stop solving a riddle, grokking into how systems work may be called …
a) a script kiddie;
b) a time-seasoned professional;

c) a walkie-talkie;
d) a puzzle junkie.

12. Which one is not likely to lead to the downfall of a cybercriminal gang?
a) jealousy;
b) feuds;
c) trust;
d) betrayal.

13. Which abbreviation is not connected with cybersecurity?
a) BAFTA;
b) OPSEC;
c) OSINT;
d) DNS.

14. Which one is not a type of cybersecurity assessment?
a) penetration testing;
b) reattack recommendation;
c) red teaming;
d) threat intelligence.

15. Which one is not a real idiom?
a) to start out on the wrong foot;
b) to raise the bar;
c) to flick a safe finger;
d) to come to the light side.

Unit 6
Supplementary exercises

Exercise 156

a. Watch the video "Cyber Crime – One of the Biggest Threats to Global Security" at https://www.youtube.com/watch?v=-DniRDbZ_Es. There are 10 factual mistakes in the transcript excerpt of the video below. Find and correct them.

CYBER CRIME – ONE OF THE BIGEST THREATS TO GLOBAL SECURITY

Why does cybersecurity matter so much? It could be because cybercrime is borderless affecting a wide range of interests targeting not only individuals but also enterprises, industries, and governments.

The growing number of cybercrime especially its role in terrorism makes it one of the biggest threats to local security. According to PwC's, global state of information security organizations around the globe are working to develop digital infrastructure to manage these threats.

69% of companies worldwide say they have had to increase spending on cyber security as their companies have digitalized. Russian companies are lagging behind in this trend a little.

Only 84 percent say they have ramped up their cyber protection. The Internet of Things has an impact on the cyber security landscape. Just less than half of companies worldwide say they will invest in a security strategy dedicated to the Internet of Things this year. But some of the strategy starts at ground level with company workers. 56% of companies worldwide currently require their employers to complete privacy training and assessment. Russian businesses are closely in line with that number.

Cyber security does more than protect company systems from fishing. It can also give businesses a competitive advantage boosting their bottom line and building brand trust. But even with a decrease in preventative measures cybercrime remains a hazard. Last year five industries worldwide including telecoms and media reported an increase in information security incidents despite their continuous investment in security. So as cyber security and privacy practices evolve in line with technological advances, what now can be done to better address cybercrimes around the world and in Russia?

b. Make a summary of the text (see p. 59).

Exercise 157

a. Watch the video "How to Know If Your Identity Has Been Stolen" at https://www.youtube.com/watch?v=lmW1NS33OK4. Fill in the gaps with the suitable words and word combinations.

hack	passwords	fraud	social security number	data breach	
commit crimes	identity theft	commit fraud	phishing attack	scams	

Identity theft happens all the time. In 2020, it is estimated that 47 % of Americans experienced financial identity theft. With almost half of the population affected you're probably wondering if (1)….. has happened to you. We'll talk about the warning signs for identity (2)……., reveal the most common types of identity (3)…… and how to check for identity theft. How does identity theft happen?

We have three of the most common types of identity theft techniques.

The first one is (4)…….. This is where you receive an email, a text, or maybe a phone call from somebody saying that they're from a tech company probing you for personal information like your (5)……., and they'll use that personal information to (6)…….

The second common type of scam is physical theft. This is where somebody can gain information from you from maybe your driver's license, your social security card, or maybe through the mail looking for credit card information, bank account numbers, and then using that information to (7)……..

The third common type of scam is a (8)……. This is where scammers can (9)……. into a company's database, or retrieve hacked information from the dark web. This information can include anything you've put onto a shopping website such as (10)……, credit card information, or social security numbers.

b. Watch the video for the second time. Enumerate 10 serious warning signs that you might be the victim of identity theft.

The first warning sign is….
Suspicious activity on…
The third warning sign is…
Warning sign number four is…
Number five..
Warning sign number six…
Warning sign number seven…
Warning sign number eight….

Warning sign number nine…
Warning sign number ten…

c. Summarize the information you have learnt.

Exercise 158

a. Study the table below. Compare the punishments for cybercrimes in the UK and the USA.

Punishments for cybercrimes in the United Kingdom	**Punishments for cybercrimes in the USA**
The punishment for cybercrimes in the United Kingdom varies depending on the type and severity of the offense. Cybercrimes are typically prosecuted under UK law, with the most common legislation being the Computer Misuse Act 1990, the Identity Theft Act 2010, and the Fraud Act 2006. Here are some examples of potential punishments for specific cybercrimes in the UK: 1. Hacking. Penalties for unauthorized access to computer systems may include imprisonment for up to two years for minor cyber offences, and up to 14 years for more serious ones. 2. Identity Theft. Penalties for identity theft in the UK may include imprisonment for up to two years for accessing personal data without permission and up to 10 years for other types of identity theft. 3. Cyber stalking. In the UK, cyberstalking may be treated as harassment and penalties may include imprisonment for up to six months or a fine.	The punishment for cybercrimes in the USA varies depending on the severity of the offense committed. Cybercrimes are typically prosecuted under federal law, which provides significant penalties for these crimes. Here are some examples of the potential punishments for specific cybercrimes in the USA: 1. Hacking. Penalties for hacking can include imprisonment for up to 5 years and fines of up to $250,000. 2. Identity Theft. Penalties for identity theft may include imprisonment for up to 15 years and fines up to $250,000. 3. Cyberstalking. Penalties for cyberstalking may include imprisonment for up to 5 years and fines up to $250,000. 4. Cyber-terrorism. Penalties for cyber-terrorism may include substantial fines and imprisonment for up to life. 5. Ransomware Attacks. Penalties for ransomware attacks may include imprisonment for up to 20 years and fines up to $500,000.

4. Cyber-terrorism. Penalties for cyberterrorism may include imprisonment for up to life. 5. Ransomware Attacks. In the UK, ransomware attacks may be prosecuted under the Computer Misuse Act or the Fraud Act, with penalties of up to ten years imprisonment. 6. Possession or distribution of child pornography. The penalties for possessing, producing or distributing child pornography in the UK can be up to a maximum of 14 years imprisonment. It is worth noting that the punishment for cybercrimes in the UK is not only limited to imprisonment, but also includes fines or other community sentences, such as electronic monitoring or community service. Moreover, UK law enforcement agencies like the National Crime Agency (NCA) and Metropolitan police, are also authorized to seize criminals' assets that are proceeds of crime, which can result in significant financial losses for the perpetrator.	6. Possession or distribution of child pornography. Penalties for possessing or distributing child pornography are severe and may include imprisonment for up to 30 years and fines up to $250,000. Overall, the penalties for cybercrimes in the USA can be severe, including lengthy prison sentences and substantial fines. Other factors, such as the severity of the crime, the extent of damage caused, and the offender's criminal history, may also be taken into consideration when determining the punishment for a cybercrime.

b. Group work. Study information in the Internet about punishments for the similar cybercrimes in Russia.

c. Share the information you have learnt with your group.

Exercise 159

a. Watch the first part (3:55 – 5:13) of the video "How the IoT is Making Cybercrime Investigation Easier" at https://www.youtube.com/watch?v=9CemONO6vrY. There are 15 factual mistakes in the transcript excerpt of the video fragment below. Find and correct them.

HOW THE IoT IS MAKING CYBERCRIME INVESTIGATION EASIER

What if I told you this was predicted forty-five years ago? I found this book, and in this book, I'll paraphrase the two highlights that I have in the pink.

Basically, what's being described as the investigators of the future, this was written in 1981, detectives of the future will need to be computer operators or very criminal (tech) savvy. I agree I also would suggest that at least 19 (90) percent of all crime today has some technology, or Internet (digital) component whether it's in the planning, the condition (commission) or the aftermath (aftercrime). Right, there's some type of digital component. Someone planned, or research their target, someone actually used crime to crack (hack) someone, or something like that, or they, boast (bragged) about it online.

The next section talks about how computers will help control (govern) our lives, and help keep us safer. We're pretty close. We have entering management systems (access control systems) that lets us into our cars, all this is managed by a stranger (computer), or some digital device.

So how can we help your best friend? Well, I'm gonna give it my best shot, I'm not really here to help your best friend, I'm here to find the truth and figure out what happened. I want to tell a story to try to lead (steer) the investigation in the right path.

So question that I ask is "Where are the victims (eyewitnesses)? Do they exist?", and maybe the better question is "Where are the real (digital) eyewitnesses?" because they truly will tell a story, once we find them.

b) Watch the whole video. Summarize the information you've learnt.

Exercise 160

a) Watch the first part (0:00 – 1:52) of the video "The Cybercrime You Never Hear About" at https://youtu.be/mCt2hzpyWZc . There are 15 factual mistakes in the transcript excerpt of the video fragment below. Find and correct them.

THE CYBERCRIME YOU NEVER HEAR ABOUT

Financial institutions go to great lengths to protect themselves against cyberattacks, but as in "Live Free or Die Hard", very little stops the elite hackers from penetrating the most sophisticated technology.

Tom Kellermann: "The hacker underground has developed various weapons in cyberspace that allow them to steal the encryption, and thus get into these systems and steal your documents. And the average losses associated with a cyber heist is $1.5 million. An average bank robbery in the physical world where you have a gun or a weapon is only $7,000 to $10,000".

This is a criminal industry with staggering rewards. In 2003, a Miami-based hacker made crime history by pulling off one of the biggest government heists of all time, but he is far less known than the likes of Bonnie and Clyde or Billy the Kid.

Hacker Alexandro Gonzalez would drive through Miami shopping district, hacking into stores' wireless networks. He wasn't stealing their money. He was fishing for bank account numbers, and he'd struck the mother load.

Chris Wysopal: "He broke into a retailer through one of their stores and got back to the corporate headquarters, where there was a lot of credit card passwords, all stored in one database in one place".

Once Gonzalez had hacked this way into the corporate minor office, he would download tens of thousands of retailers' credit card details. Gonzalez the sold the stolen credit card details on to the Western European cyber criminals. In his first year, Gonzalez stole and incredible 13.2 million payment cards from retailers across the USA. 12 months later this had increased to almost 60 million.

b) Watch the whole video. Summarize the information you've learnt.

Exercise 161

a. Watch the first part (0:00 – 2:36) of the video "The Five Laws of Cybersecurity" at https://www.youtube.com/watch?v=_nVq7f26-Uo. There are 15 grammar mistakes in the transcript excerpt of the video fragment below. Find and correct them.

THE FIVE LAWS OF CYBERSECURITY

I'd like you to consider for a moment that there is about 6,900 languages spoken on our planet daily, and these thousands of languages serve thousands of cultures, from

the most small community to the largest continent. Now, even with this vast diversity among our global population, we have some alternative languages and methods for communication that understand by everybody.

For example, the world has mathematics. If I have one apple and somebody gives me another apple, I have two apples. This is understood worldwide without fail. Now, as of today, the larger culture by far is that of the Internet user. With 7.6 billion humans on Earth, around 3.6 billion of us are online and communicating with each other and institutions daily. Thus, another common language we all share but most doesn't realize is the networking protocols that the Internet runs on and the social media platforms that tie us together – and emojis; we can't forget the emojis. But what our internet culture tends to lack is a common understanding, to foster true, true understanding about cybersecurity and threats online. Outside of hardcore cybersecurity and IT people like myself, most people aren't understanding the language that is nerd. And so, it is my job to be the most good nerd-to-English translator I can be in order to help the world stay safe online.

So, without further ado, here are my five laws of cybersecurity that design to do just that. Law number 1: If there is a vulnerability, it will exploit. No exceptions. Consider for a moment that when the first bank conceived of and built, there was at least one person out there who thinked, "I want to rob that." In the more modern era, since the first computer bug was discovered, hackers good and bad have looking for ways to get around the laws and framework that govern a computer system, a program, or even our society in general. Now, think about this for a second. There are those out there who was literally try and hack absolutely everything within their capability. Now, this could be the more basic exploit, like the person who was figured out how to cover their car's license plate to go through an automatic tollbooth for free, or this could be a more obscure, such as infecting a complex computer network to derail an entire illegal nuclear weapons program, which actually have happened in the mid-2000s. Finding ways around everything for both good and bad purposes is so ubiquitous today, we even have a term for it: life hacking.

b. Watch the whole video. Name the five laws of cybersecurity and summarize the information you've learnt.

Exercise 162

a. Watch the part (8:15 – 10:07) of the video "Digital Forensics" at https://youtu.be/Pf-JnQfAEew. There are 15 factual mistakes in the transcript excerpt of the video fragment below. Find and correct them.

A CASE FROM DIGITAL FORENSICS

I got a phone call one day and one of our clients says: “Davon, can you stop the telephone in our company?”. And this was a food company. “So, you're saying you want to stop the Internet?” There's got to be something more to it than that.

So, after a long chat with my client is they say: “Yes, we've received a letter from the environment agency that says a certain IP address in our company has breached certain policies on their backend”. And what they wanted was that a fine was to be submitted or a lawsuit wouldn't shoot. Now obviously our client was not willing to pay the fine. They realized what had happened and they were happy to pay the fine. But they said: “We want to find the bad banana. We don't want this to ever happen in our company again. I only care what the cost is.”

So again, we were asked to help them out. Now we had done no projects with this company, and a part of the work that we do as I mentioned before is to be public and to be discreet. So only two people in the organization knew what we were doing: the head of legal and the head of IT. And that's quite important. This type of discreet matters because you don't want it to be leaked out into the government.

Now how did we approach this? We knew there was an email involved and we did not know the date range. So, through logs we were able to tell that fifteen people had used this IP address previously in the company. So, what we did was we ran stealth key searches to allow us to search over the network, via the network. So, we then rock up to the person's desk and say “Hey, can I take your machine?”. We did it over the network and after a few days we had nothing.

b. Watch the whole video. Summarize the information you’ve learnt.

GRAMMAR REFERENCE

VERB TENSES – ACTIVE VOICE

	Simple	Continuous	Perfect	Perfect Continuous
Present	**V; he, she, it – V+s/es (-/? do/does)** GDPR *forces* companies to justify everything that they *do* with personal data.	**am/is/are + Ving** 1. I *am learning* new information about malware. 2. How *is* this company *securing* its critical data? 3. Today all companies *are facing* different cyber threats.	**have/has + V_3** 1. Hackers *have learned* to exploit "weak points" of different devices. 2. Cybersecurity *has become* a vital part of any sphere of modern life.	**have/has been + Ving** 1. Recent incidents *have been demonstrating* how easily malicious hackers were stealing data. 2. Each company *has been expanding* its focus on data protection for the last 20 years.
Past	**V+ed/V_2 (-/? did)** 1. Tim *uploaded* his photo to the Internet. 2. A hacker *sold* confidential information to criminals.	**was/were + Ving** 1. Ann *was shopping* online when her credit card details were stolen. 2. Cyber criminals *were looking* for ways to steal your passwords.	**had + V_3** The crime ring *had* already *collected* some information about Tim.	**had been + Ving** A lot of information was stolen because attackers *had been using* more sophisticated techniques to target the system.
Future	**will + V** In the future we *will* invent a completely secure way of communicating with each other online.	**will be +Ving** Organizations *will be paying* a lot of money to highly skilled cybersecurity professionals.	**will have + V_3** Cybersecurity experts *will have solved* the problem by tomorrow.	**will have been + Ving** I *will have been protecting* this company from cyberattacks for three years next Monday.

For more grammar practice visit the site https://onlinetestpad.com/ru/test/433633-tenses-of-english-verb-active-voice and do exercises online.

VERB TENSES – PASSIVE VOICE (BE + PAST PARTICIPLE)

	Simple	***Continuous***	***Perfect***
Present	**am/is/are + V_3** 1. I *am interested* in protecting my computer from cyber attacks. 2. The term 'cybersecurity' *is used* in a variety of contexts. 3. Individuals, small businesses, and large organizations *are* all *affected*.	**am/is/are being + V_3** 1. I *am being* trained at work. 2. The client's information *is being secured*. 3. Businesses *are being attacked* by hackers.	**have/has been + V_3** 1. The risk of cyber attacks *has been reduced*. 2. Tim's photos *have been made* available to an advertising firm.
Past	**was/were + V_3** 1. My personal data *was deleted*. 2. The company's sensitive files *were accessed* by a hacker.	**was/were being + V_3** While an employee was working, the company's sensitive data *was/were being transmitted* to the hacker's computer.	**had been + V_3** As the risk *had been identified*, it could be avoided.
Future	**will be + V_3** The computer *will be fixed*.	_____	**will have been + V_3** In three days, a new cybersecurity software *will have been installed* on our computer.

For more grammar practice visit the site: https://www.english-grammar.at/online_exercises/passive-voice/pa016.htm and do exercises online and do exercises online.

DEGREES OF COMPARISON

	Adjective	***Comparative***	***Superlative***
One syllable adj	high	**-er** high**er**	**the +adj + -er** **the** high**est**
One vowel + one consonant = double final consonant	big	big**ger**	**the** big**gest**
Two syllable adj ending in consonant + y	risky	~~**y**~~ **+ ier** risk**ier**	**the + adj-~~y~~ + iest** risk**iest**
Two or more syllables	important	**more + adj** **more** important	**the most + adj** **the most** important
Irregular adjectives	good	**better**	**the best**
	bad	**worse**	**the worst**
	far	**further / farther**	**the furthest / the farthest**

For more grammar practice visit the site: https://onlinetestpad.com/ru/test/331023-degrees-of-comparison and do exercises online.

CONDITIONALS

Study the grammar rules on the use of Conditionals.

Conditionals are sentences with two clauses, one of which is an 'if' clause, the other one is the main clause. Four basic conditionals used in English are:

- Zero Conditional;
- First Conditional;
- Second Conditional;
- Third Conditional.

Zero Conditional	***something that is always true,*** ***or something that is advised in this situation***
If + ***Present Simple***	***+ Present Simple***

If your mobile phone is stolen,	it is important that your contact the police and your service provider as soon as possible.
If cybercriminals fake the pages of Internet-banking or popular Internet-stores than,	usually, they get money directly.
If the crime is not serious,	you can also report it online on the police website.

First Conditional	***something that will possibly happen in the future***
If + ***Present Simple***	***+ Future Simple***
Even if considerable progress is made in all these areas,	organized crime and cybercrime will continue to flourish.
If you commit cyber fraud or falsify information in connection with your use of the App or Website or in connection with your account,	your account will be terminated immediately.
If someone hacks your account or if your exchange shuts down,	the government will not reimburse you for the money you lose.

Second Conditional	***something that is probably not going to happen***
If + ***Past Simple***	***+ would + Infinitive***
If the computer was already compromised,	many antivirus products won't be able to be installed or updated until the malware is removed completely.
Even if hackers and cybercriminals were to gain access to said information,	it would be of no use to them.
If our trade secrets *were materialized* in that product,	third parties *would be able to discover* them.
Third Conditional	***something that did (not) happen, and you regret that it did (not)***
If + ***Past Perfect***	***+ would + have + III form of the verb***
If he hadn't been so nervous in the interview,	he would have got a job in Yandex.
If the law had not been passed,	it would have been much more difficult to abolish constitutional guarantees.

If you had been more attentive,	you would not have become a victim of cyber fraud.

NOTE THE COMMA! When an if-clause stands first, we should separate it from a main clause by a comma. If an if-clause follows a main clause, no comma is needed.

For more grammar practice visit the site https://www.perfect-english-grammar.com/conditional-exercises.html and do exercises online.

REPORTED SPEECH

Reported speech is our representation of other people's speech or our own words. Reported speech might be separated into two main types: direct speech and indirect speech. Indirect speech focuses more on the content of what was said rather than the exact words. In indirect speech, the reported clause's structure depends on whether the speaker is reporting a statement, a question or a command.

Indirect speech. Statements

When one transforms a direct statement into indirect, one should look carefully at the verb which stands in front of the direct speech:

The judge says "The defendant is guilty" – The judge says (that) the defendant is guilty.

The judge said "The defendant is guilty" – The judge said (that) the defendant was guilty.

Two clauses are connected with the conjunction *"that"*. However, it may be omitted, especially, in informal speech.

A verb in its past form causes so-called 'backshift' in the reported clause. The tenses should be changed as follows:

Present Tenses	->	**Past Tenses**
Present Simple	->	Past Simple
Present Continuous	->	Past Continuous
Present Perfect	->	Past Perfect

Present Perfect Continuous	->	Past Perfect Continuous
Past Simple Tenses	**->**	**Past Perfect Tenses**
Past Simple	->	P. Perfect
Past Continuous	->	Past Perfect Continuous
Past Perfect\Past Perfect Continuous	->	Past Perfect\Past Perfect Continuous
Future Tenses (will)	**->**	**Future-in-the-Past Tenses (would)**

Sometimes there is no 'backshift'. It happens when the information given in indirect speech is still true or relevant or has not happened yet.

He said "The clear sky is blue" – He said (that) the clear sky is blue.

Apart from changes to tenses, adverbs and demonstratives should be also changed:

today	->	that day
tonight	->	that night
tomorrow	->	the next\following day
next (week, month, etc.)	->	the next\following (week, month, etc.)
ago	->	before
yesterday	->	the day before\the previous day
last (week, month, etc.)	->	the last\previous (week, month, etc.)
now	->	then
here	->	there
this (place)	->	that (place)

Indirect speech. Questions

The main distinctive feature of English questions is their word order. Typically, it can be described as "VSO", i.e. "verb, subject, object". When one makes any direct question indirect, one should keep the word order direct ("SVO", i.e. "subject, verb, object")

Then, one should distinguish two main types of English questions: general questions (also called yes/no questions) and special questions (wh-questions).

General questions (Yes, no questions)

Such questions may have a modal, an auxiliary verb, the verb "to be" (when a main verb) as the beginning:

Can (a modal) *I appeal the decision?*

Do (an auxiliary verb) *you work at the law school?*

Are ("to be" as a main verb) *you a barrister?*

Transforming a direct question into indirect, one should connect two clauses by means of conjunctions "whether" or "if":

I asked ***whether/if*** *I could appeal the decisions.*

I asked ***whether/if*** *you worked at the law school.*

I asked ***whether/if*** *he was a barrister.*

Note that the rule of backshift is applicable.

Special questions (Wh-questions)

The main difference betwen this type of questions and the previous type is that one does not need any word to connect clauses. On the contrary, a question word (a wh-word) is used to connect clauses.

Where *is my book? – I asked* ***where*** *my book was.*

It is necessary to distinguish subject and object questions. The words who\what may be both the subject and an object of a sentence:

Who (object) *are you talking to? – I asked* ***who*** *you were talking to.*

Who *told you that? – I asked* ***who*** *had told you that.*

Indirect speech. Commands

When it comes to reporting commands, a sentence consists of a reporting clause, and a reported clause beginning with an infinitive:

*The judge told the jury, "**Disregard** his testimony" – The judge **told** the jury **to disregard** his testimony.*

*The claimants asked the Commission, "**Focus** on the horse ID forms. please" – The claimants **asked** the Commission t**o focus** on the horse ID forms.*

We also use a *to*-infinitive clause in indirect reports with other verbs that mean wanting or getting people to do something. These verbs are called reporting verbs.

Indirect speech. Reporting verbs

Various reporting verbs require different patterns when they are used in reported speech. You can see some verbs below:

Patterns		Verbs	Examples
1. verb + that clause	no object	add, admit, announce, claim, complain, insist, reply, respond, say, state, suggest	Jack **admitted that** he had robbed that woman.

	+ object	tell someone, warn someone	A police officer **told us that** this was the apartment where the murder had taken place.
2. verb + infinitive with to	no object	agree, claim, offer, refuse	The only witness **agreed to give** her testimony.
	+ object	advise someone, ask someone, beg someone, encourage someone, invite someone, order someone, persuade someone, remind someone, tell someone, warn someone	The victim **begs the sheriff to show** mercy.
3. verb + gerund	no preposition	admit, advise, consider, regret, suggest	John **admitted killing** by restlessness.
	+ preposition	admit to, apologize for, complain about, insist on, thank someone for	More than one third of drivers **admit to breaking** ru les of road.

NB! Some reporting verbs (they are underlined in the table) have more than one pattern.

For more grammar practice visit the site https://www.english-grammar.at/online_exercises/reported-speech/reported-speech-index.htm and do exercises online.

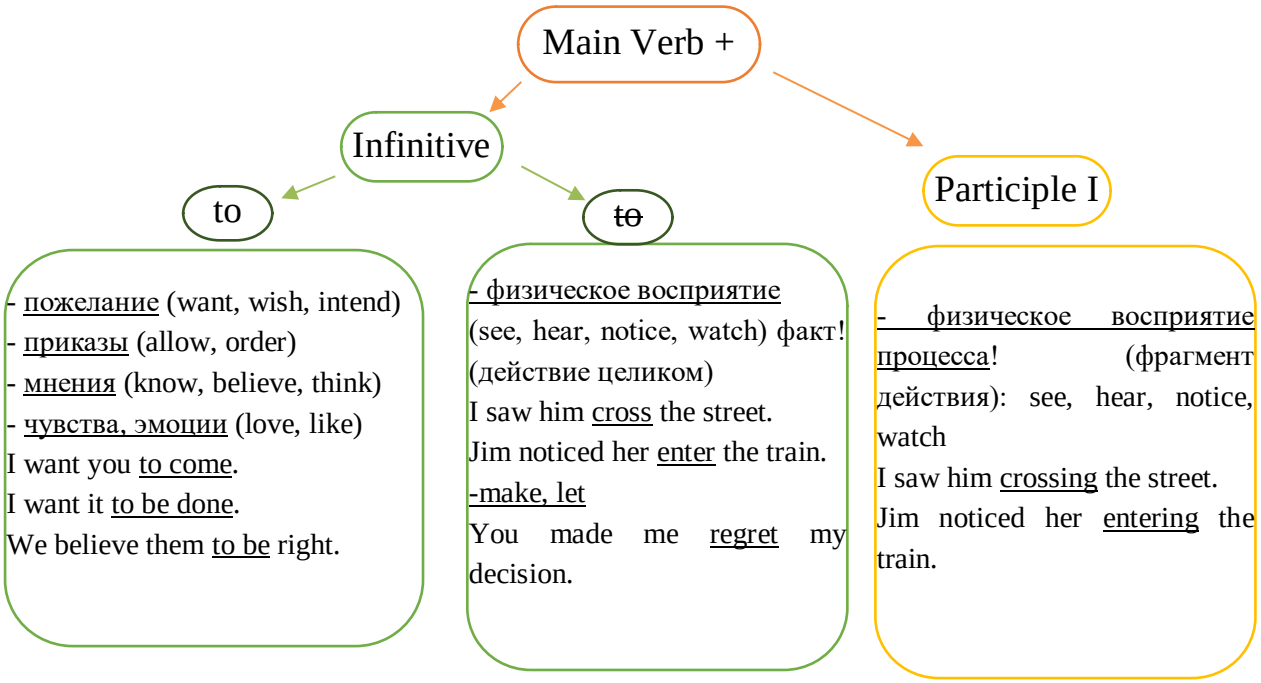
COMPLEX OBJECT

Оборот Complex Object is a structure used to make sentences more compact. It consists of:

Verb + Object + Infinitive (with or without "to") // Participle I (Ving)

I saw *him investigating* the crime.	Я видел, *как он расследовал* дело.
He *made me hack* this computer.	Он *заставил меня взломать* этот компьютер.
I *recommend you to make* backups.	Я *рекомендую вам делать* резервные копии.

To choose between the correct form of an infinitive or a participle pay attention to the **Main Verb:**



For more grammar practice visit the site: https://englika.ru/tests/test-na-complex-object and do exercises online.

COMPLEX SUBJECT

The Complex Subject in English is usually translated into Russian by such phrases as "They say, they report, they heard etc." To formulate a sentence with the Complex Subject you place a passive 'introductory' verb (…is said...) after the subject. The main action is expressed by the following Infinitive.

He is said to violate the law.

The verbs typically used with the Complex Subject may be divided into several groups:

Verbs of knowing	Verbs of supposition, expectation	Sensory verbs	Adjectives of probability
is said - говорят is known - знают is thought - думают is stated - утверждают is reported - сообщают is announced - заявляют	is expected - предполагается is believed - полагают is considered - считается is supposed – ожидают	is heard - слышали is seen - видели is noticed - замечено	is likely - вероятно is unlikely - маловероятно is certain - точно is sure – точно

Sentences with the Complex Subject may be used in the past form. Additional aspects of the expressed action should be specified by the different forms of the Infinitive.

He was said to violate the law.
He was said to be violating the law.
He was said to have violated the law.

When you need the negation you should place “not” before the Infinitive:

She is believed not to preside over the court this year.

The meaning of the Complex Subject might be equally expressed with two clauses, one of them with the ‘dummy’ subject.
It is believed that they are black-hat hackers. = They are believed to be black-hat hackers.
It was reported that the court hearing would last 2 hours = The court hearing was reported to last 2 hours.

For more grammar practice visit the site: https://englika.ru/tests/test-na-complex-subject and do exercises online.

GLOSSARY

accidental action	непреднамеренное действие
antivirus software	антивирусное ПО
to attack	атаковать, нападать
attacker	злоумышленник, взломщик, хакер
authentication	аутентификация, авторизация, проверка подлинности
to be hacked	быть взломанным
to be out of reach	быть недоступным, вне досягаемости
to be resilient against	быть устойчивым к
black-hat hacker	хакер-злоумышленник
blackmail	шантаж, вымогательство; шантажировать
breach	взлом, повреждение, утечка (данных)
brute-force attack	атака полным перебором
bug bounty	1) выявление ошибок и уязвимостей в компьютерной программе или системе (за вознаграждение) 2) вознаграждение за выявление ошибок и уязвимостей в компьютерной программе
to bypass	обойти, миновать
capacity	*юр*. дееспособность, правоспособность
chief security officer (CSO)	начальник службы безопасности
classified	не подлежащий оглашению
to close a case	закрыть дело, закончить расследование
to commit a crime	совершить преступление
to comply with	соблюдать, выполнять, соответствовать
to compromise	нарушить секретность, скомпрометировать, взломать
computer crime	преступления, связанные с использованием компьютеров
computer trespass	вторжение в частное электронное пространство
computer virus	компьютерный вирус
computer worm	компьютерный червь
con	афера

to con	обманывать
counterfeiting	изготовление контрафактной продукции
credential stuffing	подстановка учетных данных
credentials	учетные данные
criminal (adj)	уголовный (прил.
criminal (n)	преступник (сущ.)
cyber attack	кибератака
cyber defence	киберзащита
cyber defence system	система киберзащиты
cyber incident	кибератака
cyber security	кибербезопасность
cyber stalking	киберпреследование – использование интернета для преследования или домогательств человека, группы людей или организации
cyber threat	киберугроза
cybercrime investigator	следователь по делам о преступлениях в сфере IT
cybercriminal	преступник, виновный в совершении преступления в сфере IT
cybercriminal gang	банда киберпреступников
cyber-enabled, cyber-dependent	возможные благодаря киберпространству или пользующиеся киберпространством
cyberfraud	кибермошенничество
cyberintruder	хакер
cybersecurity assessment	тест кибербезопасности
damage	вред, ущерб, урон
darknet	Даркнет, «темный Интернет»
data	данные, сведения, информация
data breach	утечка данных
to deal with	иметь дело/ заниматься чем-либо
decryption key	ключ шифрования
deliberate action	умышленное действие

denial of service (DoS)	отказ в обслуживании
deterrence	сдерживание
digital	цифровой, электронный
digital (computer) forensics	цифровая (компьютерная) криминалистика
digital footprints	цифровой след
to eliminate	устранять
to encrypt	шифровать, кодировать
encryption	шифрование
enhancement	улучшение, усиление
to foil	предотвращать
forensic evidence	судебное доказательство
forensic standards	стандарты расследования
to foster	поощрять, поддерживать
fraud	мошенничество
gambling	игра на деньги/игра в азартные игры
to hack	взламывать
hacker	хакер, злоумышленник
hacker attack	хакерская атака
harassment	харассмент, домогательство, преследование
identity theft	кража персональных данных
illegal	незаконный
to implement	внедрять, применять
to infiltrate	тайно проникнуть
invasion of privacy	вмешательство в личную жизнь
to investigate	расследовать
investigation	расследование
to jeopardize	подвергать риску
leaked	слитый (о данных)
legitimate	законный, легитимный
to locate	определять точное местонахождение
logic (software) bomb	логическая бомба
to make purchases	делать покупки
malefactor	злоумышленник

malicious	злоумышленный, вредоносный
malware	вредоносное ПО
mishandling	небрежное, ненадлежащее обращение
misuse	злоупотребление, нецелевое употребление
to pass laws	принимать законы
password	пароль
patch	ПО для оперативного исправления ошибки в программе, патч («заплата»)
penetration testing	тестирование на проникновение
phishing	фишинг, обман с целью получения доступа к учетным данным
privacy	конфиденциальность
private	личный, конфиденциальный
to promote	продвигать
to put someone behind bars	посадить кого-либо за решетку
ransomware	вирус-вымогатель
reconnaissance	рекогносцировка
red teaming	имитация реальной атаки
regulation	правило, закон, регулирование
regulatory tools	нормативно-правовые инструменты
to revolve around	быть так или иначе связанным с
scam	интернет-мошенничество, обман
to scam	обманывать
to secure	защищать, охранять, обезопасить
security enhancements	усиление, укрепление безопасности (меры по усилению безопасности)
sensitive	конфиденциальный, личный, связанный с важной/секретной информацией
sexual abuse	сексуализированное насилие
smishing	смишинг, фишинг через СМС
social engineering	метод проникновения в защищенные системы, основанный на использовании социальной психологии
software	программное обеспечение (ПО)

software piracy	нарушение авторских прав на программное обеспечение
stakeholder	вовлеченная сторона
to steal	красть, воровать
to tackle	предотвращать
to takedown someone	ликвидировать (например, преступника)
third party	*юр.* сторонняя организация
threat environment	угрожающая среда
Trojan horse	троянский конь (вредоносная программа)
unauthorized access	несанкционированный, неавторизованный доступ
unlawful access	неправомерный доступ
victim	потерпевший, пострадавший, жертва
vulnerability	уязвимость
vulnerable	уязвимый, незащищенный
web jacking	незаконное получение контроля над веб-сайтом путем захвата домена
white-hat hacker	этичный хакер
to withdraw	снимать со счета

KEYS FOR THE TESTS

Unit 1

1 – c; 2 – b; 3 – a; 4 – d; 5 – c; 6 – a; 7 – d; 8 – c; 9 – b; 10 – c; 11 – c; 12 – b; 13 – d; 14 – c; 15 – a.

Unit 2

1 – c; 2 – b; 3 – b; 4 – d; 5 – a; 6 – c; 7 – b; 8 – c; 9 – a; 10 – a; 11 – b; 12 – d; 13 – c; 14 – a; 15 – b.

Unit 3

1 – b; 2 – a; 3 – d; 4 – b; 5 – b; 6 – c; 7 – a; 8 – c; 9 – d; 10 – b; 11 – a; 12 – d; 13 – a; 14 – c; 15 – b.

Unit 4

1 – c; 2 – d; 3 – c; 4 – c; 5 – a; 6 – b; 7 – a; 8 – d; 9 – b; 10 – b; 11 – a; 12 – c; 13 – a; 14 – d; 15 – d.

Unit 5

1 – c; 2 – a; 3 – d; 4 – c; 5 – a; 6 – a; 7 – a; 8 – b; 9 – a; 10 – b; 11 – d; 12 – c; 13 – a; 14 – b; 15 – c.

Ex 50(b)


K T G U Y F F R I L K F E D O
N K N I T N T H O B E R C G O
S A I N N O M H A G A B F M Y
T T T A K I O E A B Y T G R I
R A T B F T S G N D G M G G C
A C A Q A A N I U O N N N A Y
N O U F H M A A R T I I I M B
A P Q F A A R Y F F T L K B E
H Y S I R F N R F U A F C L R
K R R R A E G I T F E A A I S
M I E S S D N N R I H T J N T
G G B I S S I G A O C Y B G A
D H Y S M T F I F A R R E W L
R T C H E A O A F N H E W C K
R O C I N P O A I M G G S A I
F E F I T G P G C D A R R A N
I M S E N M S G K P B O T I G
U O G K G R S U I A A F T F I
I M N T L N I F N F W N U F T
P R I I G A F O G I C E R G A

WEBSITE RESOURCES

1. https://alchetron.com/Kristina-Svechinskaya

2. https://businessinsights.bitdefender.com/foiling-cybercrime-around-the-world-an-interview-with-a-cybercrime-investigator

3. https://epic.org/documents/van-buren-v-united-states/

4. https://gatefy.com/blog/real-and-famous-cases-ransomware-attacks/

5. https://iosentrix.com/blog/How-OSINT-is-used-in-Cybersecurity-Part-1/

6. https://lawpage.in/cyber_laws/crime/characteristics

7. https://online.maryville.edu/blog/cyber-crime-investigation/

8. https://portswigger.net/daily-swig/us-computer-fraud-and-abuse-act-what-the-landmark-van-buren-ruling-means-for-security-researchers

9. https://techframework.com/kristina-svechinskaya-worlds-most-notorious-cyber-bank-robber/

10. https://time.com/4393372/james-comey-fbi-hillary-clinton-email-speech-transcript/

11. https://warbletoncouncil.org/hackers-famosos-1246

12. https://www.aura.com/learn/identity-theft-stories-cases

13. https://www.bbc.co.uk/news/technology-60953527

14. https://www.bbc.com/news/technology-56901364

15. https://www.blackhatethicalhacking.com/articles/hacking-stories/albert-gonzalez-the-get-rich-or-die-trying-crew-who-stole-130-million-credit-card-numbers/

16. https://www.blackhatethicalhacking.com/articles/hacking-stories/kevin-poulsen-dark-dante-and-his-hacking-activities-on-arpanets-networks/

17. https://www.blackhatethicalhacking.com/articles/how-do-qr-codes-work-and-how-criminal-hackers-use-them-to-generate-phishing-attacks-demo/

18. https://www.blackhatethicalhacking.com/articles/operation-oprussia-anonymous-attacks-on-russia/

19. https://www.businessinsider.com/kristina-svechinskaya-verdict-in-spring-2013-

20. https://www.cbc.ca/news/science/how-to-stay-safe-with-a-smartphone-1.2553592

21. https://www.easytechjunkie.com/what-is-cybercrime.htm

22. https://www.english-grammar.at/online_exercises/reported-speech/reported-speech-index.htm

23. https://www.fbi.gov/news/stories/a-byte-out-of-history-10-million-hack

24. https://www.ftc.gov/system/files/attachments/cybersecurity-small-business/cybersecuirty_sb_factsheets_all.pdf

25. https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know

26. https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-a-florida-teen-hacks-the-department-of-defense-and-nasa/

27. https://www.itgovernance.eu/blog/en/the-5-biggest-phishing-scams-of-all-time

28. https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

29. https://www.kaspersky.com/resource-center/threats/top-ten-greatest-hackers

30. https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime

31. https://www.ncsc.gov.uk/guidance/shopping-online-securely

32. https://www.ncsc.gov.uk/news/ncsc-ceo-meets-with-cyber-security-leaders-in-india

33. https://www.perfect-english-grammar.com/conditional-exercises.html

34. https://www.phonexia.com/blog/the-4-biggest-identity-theft-frauds-in-modern-history/

35. https://www.simplilearn.com/introduction-to-cyber-security-article

36. https://www.state.gov/cybercrime

37. https://www.statista.com/topics/7335/information-security-and-cyber-crime-in-russia/#topicOverview

38. https://www.stickmancyber.com/cybersecurity-blog/incident-response-frameworks-nist-sans

39. https://www.wired.co.uk/

40. https://www.youtube.com/watch?v=_nVq7f26-Uo

41. https://www.youtube.com/watch?v=-DniRDbZ_Es

42. https://www.youtube.com/watch?v=23va1vj41Zc

43. https://www.youtube.com/watch?v=9CemONO6vrY

44. https://www.youtube.com/watch?v=9TRR6lHviQc&t=27s

45. https://www.youtube.com/watch?v=aArb68OBFPg

46. https://www.youtube.com/watch?v=FsXlThlI7Ic)

47. https://www.youtube.com/watch?v=H0I7jQb37bo

48. https://www.youtube.com/watch?v=j6wwBqfSk-o

49. https://www.youtube.com/watch?v=lbCh94nJqIo&t=1s

50. https://www.youtube.com/watch?v=lmW1NS33OK4

51. https://www.youtube.com/watch?v=Ls8jyO46bmI

52. https://www.youtube.com/watch?v=Nez-niwd63Y

53. https://www.youtube.com/watch?v=QJdYjNCKCj4&t=473s

54. https://www.youtube.com/watch?v=zHmdOeQbjHA

55. https://www.youtube.com/watch?v=ZUqzcQc_syE

56. https://youtu.be/8CV1f6a9b-c

57. https://youtu.be/mCt2hzpyWZc

58. https://youtu.be/Pf-JnQfAEew

59. https://youtu.be/x0tL4U22SI8

60. https://www.technotification.com/2016/06/female-hackers-in-the-world.html

61. https://www.washingtonpost.com/business/2018/11/30/marriott-discloses-massive-data-breach-impacting-million-guests/

62. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

63. https://www.theguardian.com/technology/2022/sep/15/uber-computer-network-hack-report

64. https://aris-journal.com/aris/index.php/journal/article/view/20/16

65. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade

BIBLIOGRAPHY

1. Английский язык для юристов: учебник для академического бакалавриата/ под ред. Юговой М.А. – М: Юрайт, 2018.

2. Английский язык для юристов: Учебник / К. М. Левитан, С. В. Павлова, М. С. Пестова [и др.]; Под ред. К.М. Левитана. – Москва: Общество с ограниченной ответственностью "Издательство "КноРус", 2021. – 552 с. – (Аспирантура и магистратура).

3. Гураль С.К., Смокотин В.М., Майер Л.Г. Law and Law Enforcement: учебное пособие. Составитель. – Томск: Издательство Томского университета, 2006.

4. Фролова И.Е. English Law for Students of English / Английское право для изучающих английский язык. – Москва: Кругъ, 2010.

5. Carter D.L. Computer Crime Categories. How Techno-criminals Operate. FBI Law Enforcement Bulletin. July 1995, Vol. 64, Number 7. pp 22-23.

6. Koops B.J. Cybercrime legislation in the Netherlands // BJ Koops, Netherlands Reports To The Eighteenth International Congress Of Comparative Law. – 2010. C. 595-633.

7. MacKenzie I. English for Business Studies, Third Edition. Cambridge University Press, 2010.

8. Miller R. Business Law Today, South-Western, Cengage Learning, 2014.

9. Miller R.H. Law School Confidential. – NY., 2011.

10. Rivlin G. Understanding the Law, University Press, 2006.