Федеральное агентство по рыболовству
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Калининградский государственный технический университет»
(ФГБОУ ВО «КГТУ»)

УТВЕРЖДАЮ
И.о. директора института

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
ФГБОУ ВО «КГТУ»
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Сертификат:
4ae0684d0d529bb9d0248a5b51302ea1
Владелец: Гоконаев Мирослав Валерьевич
Действителен: с 02.08.2024 по 26.10.2025

Фонд оценочных средств

(приложение к рабочей программе дисциплины)

«ИНОСТРАННЫЙ ЯЗЫК»

основной профессиональной образовательной программы специалитета

по специальности

10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Специализация:

«БЕЗОПАСНОСТЬ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ»

ИНСТИТУТ цифровых технологий
РАЗРАБОТЧИК кафедра иностранных языков

1 РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ, ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ И КРИТЕРИИ ОЦЕНИВАНИЯ

1.1 Результаты освоения дисциплины

Таблица 1 – Планируемые результаты обучения по дисциплине, соотнесенные с установленными компетенциями

Код и наименование компетенции	Дисциплина	Результаты обучения (владения, умения и знания), соотнесенные с компетенциями
УК-4: Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)	Иностранный язык	*Знать*: иностранный язык в объёме, необходимом для получения информации общекультурного содержания из зарубежных источников. *Уметь:* начинать/вести/поддерживать и заканчивать диалог-расспрос об увиденном, прочитанном, диалог - обмен мнениями и диалог - интервью/собеседование при приеме на работу, соблюдая нормы речевого этикета, при необходимости используя стратегии восстановления сбоя в процессе коммуникации (переспрос, перефразирование и др.); высказывать свое мнение, просьбу; отвечать на предложение собеседника (принятие предложения или отказ); делать сообщения и выстраивать монолог-описание, монолог-повествование и монолог-рассуждение. *Владеть*: грамматическими навыками, необходимыми для коммуникации на иностранном языке без искажения смысла в письменной и устной форме.

1.2. К оценочным средствам текущего контроля успеваемости относятся:

- тестовые задания открытого и закрытого типов.

Промежуточная аттестация в форме зачета/экзамена, в зависимости от семестра обучения, проходит по результатам прохождения всех видов текущего контроля успеваемости. В отдельных случаях (при не прохождении всех видов текущего контроля) зачет может быть проведен в виде тестирования.

1.3 Критерии оценки результатов освоения дисциплины

Универсальная система оценивания результатов обучения включает в себя системы оценок: 1) «отлично», «хорошо», «удовлетворительно», «неудовлетворительно»; 2) «зачтено», «не зачтено»; 3) 100 – балльную/процентную систему и правило перевода оценок в пятибалльную систему (табл. 2).

Таблица 2 – Система оценок и критерии выставления оценки

Система оценок / Критерий	**2**	**3**	**4**	**5**
	0-40%	**41-60%**	**61-80 %**	**81-100 %**
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
	«не зачтено»	**«зачтено»**		
1 Системность и полнота знаний в отношении изучаемых объектов	Обладает частичными и разрозненными знаниями, которые не может научно- корректно связывать между собой (только некоторые из которых может связывать между собой)	Обладает минимальным набором знаний, необходимым для системного взгляда на изучаемый объект	Обладает набором знаний, достаточным для системного взгляда на изучаемый объект	Обладает полнотой знаний и системным взглядом на изучаемый объект
2 Работа с информацией	Не в состоянии находить необходимую информацию, либо в состоянии находить отдельные фрагменты информации в рамках поставленной задачи	Может найти необходимую информацию в рамках поставленной задачи	Может найти, интерпретировать и систематизировать необходимую информацию в рамках поставленной задачи	Может найти, систематизировать необходимую информацию, а также выявить новые, дополнительные источники информации в рамках поставленной задачи
3 Научное осмысление изучаемого явления, процесса, объекта	Не может делать научно корректных выводов из имеющихся у него сведений, в состоянии проанализировать только некоторые из имеющихся у него сведений	В состоянии осуществлять научно корректный анализ предоставленной информации	В состоянии осуществлять систематический и научно корректный анализ предоставленной информации, вовлекает в исследование новые релевантные задаче данные	В состоянии осуществлять систематический и научно-корректный анализ предоставленной информации, вовлекает в исследование новые релевантные поставленной задаче данные, предлагает новые ракурсы поставленной задачи

Система оценок / Критерий	2	3	4	5
	0-40%	41-60%	61-80 %	81-100 %
	«неудовлетворительно»	«удовлетворительно»	«хорошо»	«отлично»
	«не зачтено»	«зачтено»		
4 Освоение стандартных алгоритмов решения профессиональных задач	В состоянии решать только фрагменты поставленной задачи в соответствии с заданным алгоритмом, не освоил предложенный алгоритм, допускает ошибки	В состоянии решать поставленные задачи в соответствии с заданным алгоритмом	В состоянии решать поставленные задачи в соответствии с заданным алгоритмом, понимает основы предложенного алгоритма	Не только владеет алгоритмом и понимает его основы, но и предлагает новые решения в рамках поставленной задачи

2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Компетенция УК-4: способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)

Английский язык (1 курс)

Задания закрытого типа

1. **Read the text about friendships in the twenty-first century. Choose the correct answers from the words in *italics*.**

Friendship in the twenty-first century

In a world driven by technology that seems to have no limits, what [1] ***was happening / is happening / had happened*** to true friendship? Is it dying out or is social media such as Facebook, Twitter and LinkedIn simply changing our modern-day idea of friendship? And if so, what [2] ***does this mean / did that mean / has this meant*** for us?

As I [3] ***am writing / have written / had written*** in this blog many times, the influence of social media allows us to become more technologically connected. Yet, we [4] ***feel / want / seem*** to be losing other more important relationships. I'd even say that we're actually losing our friends.

According to recent research, the average American has only two close friends with whom they feel they

[5] ***make friends / trust someone / have a lot in common***, and around 25% [6] ***admit / tell / inform*** that they don't have any friends at all. At the same time, we [7] ***had become / were becoming / have become*** a society with a huge number of so-called 'friends' that we've been promised through Facebook and other sites.

Aristotle, the famous Greek philosopher, once asked the people of Athens, 'Who [8] ***had to / could / must*** live without friends, even if they had every other thing?' Importantly, he [9] ***believed / had believed / has believed*** that good friends were far better than any material possessions a person might have. Stop and think, then, for a moment about the quality of relationships with people we only ever meet online, and compare this with the friends we see face-to-face regularly. Which of these types of

friends do you have a deeper
[10] ***achievement / connection / happiness*** with? Which ones are really important in your life?

Ответы

1 is happening 2 does this mean 3 have written 4 seem 5 have a lot in common 6 admit 7 have become 8 could 9 believed 10 connection

2. Read the text about storytelling. Match the paragraphs A–E to the descriptions 1–5.

The art of storytelling

A There are many reasons why people have always told, and still tell, stories. They can be used to explain difficult ideas or common messages and bring communities together. Things that people have found scary, annoying or desirable have all been turned into stories by people who wanted to be sure that others felt the same. Stories have also long been used to explain how the world works and how we should behave. Many of them also explain what will happen if we do not behave appropriately; the terrible things that happen to some characters are usually caused by their own bad behaviour.

B Long before the invention of TV and radio, or computers and iPods, people entertained themselves by telling each other stories. And storytelling is not unique to any one culture. Most people enjoy a good story and storytellers from all around the world have answered this need for thousands of years. Many of us have a favourite story from childhood and very often these can be frightening and fascinating. And there are many different kinds of stories, including myths and legends, but how are they different from each other?

C A legend is a partly true story which has been handed on from person to person, and which has an important meaning for the culture which it comes from. A legend usually contains some truth, or is based around historic facts, but with extra qualities added. They often include the particular beliefs of the culture which they belong to. Legends can involve great heroes like King Arthur, unlikely creatures such as the Loch Ness Monster, or fantastic places like the lost island of Atlantis or the imaginary city of El Dorado.

D A myth, on the other hand, is a story that has a meaning deeper than the story itself. Myths usually 'explain a truth', rather than necessarily recording a true event, and so they are often used to explain how certain things have come about. For example, they may explain how the elephant got its trunk, why it rains, or why the sun rises every day and so on. The power of the meaning behind the stories, rather than the stories themselves, is the reason why certain myths continue to exist, sometimes for thousands of years.

E So how much truth is there in a myth or legend? Imagine a line that begins with accurate historical facts at one end and myths or legends at the other. As you move along the line towards the myths and legends, the facts become less important, and the meaning behind the story becomes more important. So by the time you reach the far end of the line, the story has often got a life of its own and the original facts have disappeared, or can no longer be recognized.

Which paragraph …

1 mentions an animal that probably doesn't exist? _____
2 explains why the truth behind a story often gets lost? _____
3 gives a general explanation for storytelling? _____
4 explains why some stories have been told for a very long time? _____
5 says that people from all times and places tell and listen to stories? _____

Ответы 1 C 2 E 3 A 4 D 5 B

3. **Read the text again and complete the notes. Use one word from the text for each answer.**
   - In some stories, the characters' [1] _____ causes bad things to happen to them.
   - Storytelling can be found in every [2] _____.
   - There are many different types of stories, including myths and legends.
   - Atlantis and El Dorado are examples of imaginary [3] _____ from legends.
   - Myths often explain why things happen and aren't about a real [4] _____.
   - Some stories survive for thousands of years. In myths and legends, the facts are less important than the story's [5] _____.

Ответы 1 behaviour 2 culture 3 places 4 event 5 meaning

4. **Here are four people talking about eating out. After you read, answer each question with a paragraph number (1-4).**

1.The last time I went to a restaurant was about 2 months ago. My wife and I wanted to celebrate our wedding anniversary with a good meal so we went to an expensive Italian restaurant in downtown Lisbon. We both had pasta to start and for the main course my wife ordered a steak and I chose fish. For dessert we both ate chocolate cake topped with fresh cream. Delicious!
2. I went to a restaurant yesterday evening with my sister's children. It wasn't very expensive and the menu was very limited. We all had a burger and French fries, and drank cola. It wasn't very good.
3. My boyfriend loves spicy food so this restaurant was perfect. The waiters were all really friendly and polite, and they played traditional sitar music which was very relaxing. The menu offered vegetarian dishes as well as meat dishes served with rice and a sauce - it depended on how hot you wanted it! I chose a mild beef curry but my boyfriend had a lamb 'vindaloo' - he also drank 2 liters of water!!
4. My class at the university went there last weekend. It's a very popular type of restaurant in my country. It generally offers one type of food (a kind of bread with cheese and tomato sauce) which you then choose what ingredients to add on top of it. I asked for olives and mushrooms on mine and my classmates each had something different so we could taste a piece of each person's meal.

1. In which text did the person go there for a special occasion?
2. In which text did the person visit an Indian restaurant?
3. In which text did the person eat pizza?
4. In which text did the person eat fast food?
5. In which text did someone eat seafood?
6. In which text did the person talk about the atmosphere of the restaurant?
7. Which restaurant was cheap?
8. In which text didn't the person enjoy their meal?
9. In which text did someone eat a very hot dish?
10. In which text did the person have a vegetarian meal?

5. **Match the phrasal verbs with their meanings:**

A. Look up 1. To search for information
B. Come across 2. To find unexpectedly
C. Turn down 3. To reject an offer or proposal

Ответы: A - 1, B - 2, C – 3

6. **Choose the correct word to complete the sentence:**
The movie was ___ that we couldn't finish watching it.
a) so boring
b) such boring
c) so bored
d) such bored
Ответ: a) so boring

7. **Choose the correct options that complete the sentence:**
She was _ tired _ she fell asleep on the couch.
a) too, that
b) so, that
c) enough, so
d) very, so
Ответ: b) so, that

8. **Select the words that are adjectives:**
a) quickly
b) happy
c) slowly
d) beautifully
Ответ: b) happy, d) beautifully

9. **Arrange the following steps in the correct order to install a mobile app:**
a) Search for the app you want to install.
b) Wait for the app to download and install on your device.
c) Once installed, tap the app icon to open it.
d) Open the app store on your device.
e) Tap the "Install" button next to the app.
Ответ: D A E B C

10. **Arrange the following steps in the correct order to uninstall a mobile app:**
a) Select "Uninstall" or "Delete" from the options that appear.
b) Tap and hold the app's icon on your home screen.
c) The app will be removed from your device.
d) Confirm the action when prompted.
Ответ: B A D C

11. **Arrange the following steps in the correct order to update an app on your device:**
a) Wait for the app to download and install the update.
b) Go to the "Updates" section, usually found in the bottom menu.
c) Tap the "Update" button next to the app.
d) Find the app you want to update in the list of available updates.
e) Open the app store on your device.
Ответ: E B D C A

12. Circle the incorrect **response.**

Tony	Holiday cancelled. Not happy!
Kristine	Bad luck! / I'm so jealous! / Sorry to hear that.
Marta	Just arrived to the airport. Barbados here we come!
Sarah	You lucky thing! / Have a fab time! / Get well soon.
Mary	Great news – won my tennis match!
John	Congratulations! / Thinking of you. / Well done!

Ответы: 1. I'm so jealous! 2. Get well soon. 3. Thinking of you.

Задания открытого типа

13. You recently had an unusual or exciting experience. Write a diary entry or online blog about it. Write 120–150 words.

You should:

- say what happened
- use time expressions to show the order of events
- use comment adverbs to say how you felt about it.

14. For tasks 13- 18 complete the following sentences with the appropriate words:

She ___ to the store when she realized she forgot her wallet.

Ответ: headed

15. The concert was so ___ that everyone had a great time.

Ответ: exciting

16. He _____to answer the question because he wasn't sure of the right response.

Ответ: hesitated

17. The children were _____to go to the amusement park for the first time. **Ответ:** excited

18. Despite feeling unwell, she _____on attending the important meeting. **Ответ:** insisted

19. The team _____their victory with a party at their captain's house.

Ответ: celebrated

20. Write a paragraph about your free time, answering the following questions.

- What is your favourite free-time activity?
- How often do you use your computer?
- What do you use the computer for?
- How often do you watch TV?
- Do you think you spend your free time well? Why/Why not

21. For tasks 21-32 complete the sentences with one word only.

She usually goes clubbing with some friends _____ love dancing.

Ответ: who

22. I do exercise _____ or twice a week.

Ответ: once

23. What _____ of car do you drive?

Ответ: kind

24. He's driving _____ the moment so he can't talk on the phone.

Ответ: at

25. My parents go on a trip _____ month.

Ответ: every

26. How _____ do you have a family meal?

Ответ: often

27. There were very _____people at the party when we arrived but half an hour later, it was crowded.

Ответ: few

28. How was I to know that she would have an allergic reaction _____the nuts in the cake? She should have said something!

Ответ: to

29. You were driving at over fifty miles _____ hour and the limit here is only forty.

Ответ: per / an.

30. I _____to go to school now, otherwise I will be late.

Ответ: have / ought / need.

31. I can eat almost _____type of fish or seafood except for octopus which I can't stand.

Ответ: any

32. The city is pretty safe although you may have some problems if you go into certain neighborhoods _____ night.

Ответ: at

33. Give an appropriate response

Eldon: Driving test tomorrow…

You: _____

Ответ: Good luck / Best of luck! / Fingers crossed!

34. Think of an appropriate reaction:

Jill: Bad back – can't move!

Stuart: _____

Ответ: Get well soon / Hope you feel better soon.

35. You should listen to the advice _____ you feel it will benefit you. **Ответ:** if.

36. The door to the secret room was hidden _____a large bookcase.

Ответ: behind.

37. The performance was _____ good that they decided to see it again the following night.

Ответ: so.

38. Sarah wanted to try _____the new recipe she found in a magazine. **Ответ:** out.

39. On her holiday, she _____ across a beautiful hidden beach.

Ответ: came.

40. The new policy isn't fair _____ all employees, so it needs to be revised.

Ответ: for / on / to.

41. The students were divided _____four different teams.

Ответ: into.

Английский язык (2 курс)

Экзаменационные билеты:

Задания 1- 10

Прочитайте, переведите и изложите устно основное содержание прочитанного.

1

Information security (sometimes referred to as InfoSec) covers the tools and processes that organizations use to protect information. This includes policy settings that prevent unauthorized people from accessing business or personal information. InfoSec is a growing and evolving field that covers a wide range of fields, from network and infrastructure security to testing and auditing.

Information security protects sensitive information from unauthorized activities, including inspection, modification, recording, and any disruption or destruction. The goal is to ensure the safety and privacy of critical data such as customer account details, financial data or intellectual property.

The consequences of security incidents include theft of private information, data tampering, and data deletion. Attacks can disrupt work processes and damage a company's reputation, and also have a tangible cost.

Organizations must allocate funds for security and ensure that they are ready to detect, respond to, and proactively prevent, attacks such as phishing, malware, viruses, malicious insiders, and ransomware.

The basic tenets of information security are confidentiality, integrity and availability. Every element of the information security program must be designed to implement one or more of these principles. Together they are called the CIA Triad.

Confidentiality measures are designed to prevent unauthorized disclosure of information. The purpose of the confidentiality principle is to keep personal information private and to ensure that it is visible and accessible only to those individuals who own it or need it to perform their organizational functions.

Integrity

Consistency includes protection against unauthorized changes (additions, deletions, alterations, etc.) to data. The principle of integrity ensures that data is accurate and reliable and is not modified incorrectly, whether accidentally or maliciously.

Availability

Availability is the protection of a system's ability to make software systems and data fully available when a user needs it (or at a specified time). The purpose of availability is to make the technology infrastructure, the applications and the data available when they are needed for an organizational process or for an organization's customers.

2

Information Security vs Cybersecurity

Information security differs from cybersecurity in both scope and purpose. The two terms are often used interchangeably, but more accurately, cybersecurity is a subcategory of information security. Information security is a broad field that covers many areas such as physical security, endpoint security, data encryption, and network security. It is also closely related to information assurance, which protects information from threats such as natural disasters and server failures.

Cybersecurity primarily addresses technology-related threats, with practices and tools that can prevent or mitigate them. Another related category is data security, which focuses on protecting an organization's data from accidental or malicious exposure to unauthorized parties.

An Information Security Policy (ISP) is a set of rules that guide individuals when using IT assets. Companies can create information security policies to ensure that employees and other users follow security protocols and procedures. Security policies are intended to ensure that only authorized users can access sensitive systems and information.

Creating an effective security policy and taking steps to ensure compliance is an important step towards preventing and mitigating security threats. To make your policy truly effective, update it

frequently based on company changes, new threats, conclusions drawn from previous breaches, and changes to security systems and tools.

Make your information security strategy practical and reasonable. To meet the needs and urgency of different departments within the organization, it is necessary to deploy a system of exceptions, with an approval process, enabling departments or individuals to deviate from the rules in specific circumstances.

Top Information Security Threats

There are hundreds of categories of information security threats and millions of known threat vectors. Below we cover some of the key threats that are a priority for security teams at modern enterprises.

The speed and technological development often leads to compromises in security measures. In other cases, systems are developed without security in mind, and remain in operation at an organization as legacy systems. Organizations must identify these poorly secured systems, and mitigate the threat by securing or patching them, decommissioning them, or isolating them.

3

Many people have social media accounts, where they often unintentionally share a lot of information about themselves. Attackers can launch attacks directly via social media, for example by spreading malware via social media messages, or indirectly, by using information obtained from these sites to analyze user and organizational vulnerabilities, and use them to design an attack.

Social engineering involves attackers sending emails and messages that trick users into performing actions that may compromise their security or divulge private information. Attackers manipulate users using psychological triggers like curiosity, urgency or fear. Because the source of a social engineering message appears to be trusted, people are more likely to comply, for example by clicking a link that installs malware on their device, or by providing personal information, credentials, or financial details.

Organizations can mitigate social engineering by making users aware of its dangers and training them to identify and avoid suspected social engineering messages. In addition, technological systems can be used to block social engineering at its source, or prevent users from performing dangerous actions such as clicking on unknown links or downloading unknown attachments.

Malware on Endpoints: Organizational users work with a large variety of endpoint devices, including desktop computers, laptops, tablets, and mobile phones, many of which are privately owned and not under the organization’s control, and all of which connect regularly to the Internet.

A primary threat on all these endpoints is malware, which can be transmitted by a variety of means, can result in compromise of the endpoint itself, and can also lead to privilege escalation to other organizational systems.

Traditional antivirus software is insufficient to block all modern forms of malware, and more advanced approaches are developing to securing endpoints, such as endpoint detection and response (EDR).

Encryption processes encode data so that it can only be decoded by users with secret keys. It is very effective in preventing data loss or corruption in case of equipment loss or theft, or in case organizational systems are compromised by attackers.

Unfortunately, this measure is often overlooked due to its complexity and lack of legal obligations associated with proper implementation. Organizations are increasingly adopting encryption, by purchasing storage devices or using cloud services that support encryption, or using dedicated security tools.

4

Modern organizations use a huge number of technological platforms and tools, in particular web applications, databases, and Software as a Service (SaaS) applications, or Infrastructure as a Service (IaaS) from providers like Amazon Web Services.

Enterprise grade platforms and cloud services have security features, but these must be configured by the organization. Security misconfiguration due to negligence or human error can result in a security breach. Another problem is “configuration drift”, where correct security configuration can quickly become out of date and make a system vulnerable, unbeknownst to IT or security staff.

Organizations can mitigate security misconfiguration using technological platforms that continuously monitor systems, identify configuration gaps, and alert or even automatically remediate configuration issues that make systems vulnerable.

Information security is intended to protect organizations against malicious attacks. There are two primary types of attacks: active and passive. Active attacks are considered more difficult to prevent, and the focus is on detecting, mitigating and recovering from them. Passive attacks are easier to prevent with strong security measures.

An active attack involves intercepting a communication or message and altering it for malicious effect. There are three common variants of an active attacks:

- Interruption—the attacker interrupts the original communication and creates new, malicious messages, pretending to be one of the communicating parties.
- Modification—the attacker uses existing communications, and either replays them to fool one of the communicating parties, or modifies them to gain an advantage.
- Fabrication—creates fake, or synthetic, communications, typically with the aim of achieving denial of service (DoS). This prevents users from accessing systems or performing normal operations.

In a passive attack, an attacker monitors, monitors a system and illicitly copies information without altering it. They then use this information to disrupt networks or compromise target systems.

The attackers do not make any change to the communication or the target systems. This makes it more difficult to detect. However, encryption can help prevent passive attacks because it obfuscates the data, making it more difficult for attackers to make use of it.

5

Information security, sometimes shortened to InfoSec, is the practice of protecting information by mitigating information risks. It is part of information risk management. It typically involves preventing or reducing the probability of unauthorized/inappropriate access to data, or the unlawful use, disclosure, disruption, deletion, corruption, modification, inspection, recording, or devaluation of information. It also involves actions intended to reduce the adverse impacts of such incidents. Protected information may take any form, e.g. electronic or physical, tangible (e.g. paperwork) or intangible (e.g. knowledge). Information security's primary focus is the balanced protection of the confidentiality, integrity, and availability of data (also known as the CIA triad) while maintaining a focus on efficient policy implementation, all without hampering organization productivity. This is largely achieved through a structured risk management process that involves:

- identifying information and related assets, plus potential threats, vulnerabilities, and impacts;
- evaluating the risks
- deciding how to address or treat the risks i.e. to avoid, mitigate, share or accept them
- where risk mitigation is required, selecting or designing appropriate security controls and implementing them
- monitoring the activities, making adjustments as necessary to address any issues, changes and improvement opportunities.

To standardize this discipline, academics and professionals collaborate to offer guidance, policies, and industry standards on password, antivirus software, firewall, encryption software, legal liability, security awareness and training, and so forth. This standardization may be further driven by a wide variety of laws and regulations that affect how data is accessed, processed, stored, transferred and destroyed. However, the implementation of any standards and guidance within an entity may have limited effect if a culture of continual improvement isn't adopted.

Various definitions of information security are suggested. For example:

"Information Security is a multidisciplinary area of study and professional activity which is concerned with the development and implementation of security mechanisms of all available types (technical, organizational, human-oriented and legal) in order to keep information in all its locations (within and outside the organization's perimeter) and, consequently, information systems, where information is created, processed, stored, transmitted and destroyed, free from threats.

6

At the core of information security is information assurance, the act of maintaining the confidentiality, integrity, and availability (CIA) of information, ensuring that information is not compromised in any way when critical issues arise. These issues include but are not limited to natural disasters, computer/server malfunction, and physical theft. While paper-based business operations are still prevalent, requiring their own set of information security practices, enterprise digital initiatives are increasingly being emphasized, with information assurance now typically being dealt with by information technology (IT) security specialists. These specialists apply information security to technology (most often some form of computer system). It is worthwhile to note that a computer does not necessarily mean a home desktop. A computer is any device with a processor and some memory. Such devices can range from non-networked standalone devices as simple as calculators, to networked mobile computing devices such as smartphones and tablet computers. IT security specialists are almost always found in any major enterprise/establishment due to the nature and value of the data within larger businesses. They are responsible for keeping all of the technology within the company secure from malicious cyber attacks that often attempt to acquire critical private information or gain control of the internal systems.

The field of information security has grown and evolved significantly in recent years. It offers many areas for specialization, including securing networks and allied infrastructure, securing applications and databases, security testing, information systems auditing, business continuity planning, electronic record discovery, and digital forensics. Information security professionals are very stable in their employment. As of 2013 more than 80 percent of professionals had no change in employer or employment over a period of a year, and the number of professionals is projected to continuously grow more than 11 percent annually from 2014 to 2019.

Threats

Information security threats come in many different forms. Some of the most common threats today are software attacks, theft of intellectual property, theft of identity, theft of equipment or information, sabotage, and information extortion. Viruses, worms, phishing attacks, and Trojan horses are a few common examples of software attacks. The theft of intellectual property has also been an extensive issue for many businesses in the information technology (IT) field.

7

Threats

Information security threats come in many different forms. Some of the most common threats today are software attacks, theft of intellectual property, theft of identity, theft of equipment or information,

sabotage, and information extortion. Viruses,[39] worms, phishing attacks, and Trojan horses are a few common examples of software attacks. The theft of intellectual property has also been an extensive issue for many businesses in the information technology (IT) field.

Identity theft is the attempt to act as someone else usually to obtain that person's personal information or to take advantage of their access to vital information through social engineering. Theft of equipment or information is becoming more prevalent today due to the fact that most devices today are mobile, are prone to theft and have also become far more desirable as the amount of data capacity increases. Sabotage usually consists of the destruction of an organization's website in an attempt to cause loss of confidence on the part of its customers. Information extortion consists of theft of a company's property or information as an attempt to receive a payment in exchange for returning the information or property back to its owner, as with ransomware. There are many ways to help protect yourself from some of these attacks but one of the most functional precautions is conduct periodical user awareness. The number one threat to any organisation are users or internal employees, they are also called insider threats.

Governments, military, corporations, financial institutions, hospitals, non-profit organisations, and private businesses amass a great deal of confidential information about their employees, customers, products, research, and financial status. Should confidential information about a business's customers or finances or new product line fall into the hands of a competitor or a black hat hacker, a business and its customers could suffer widespread, irreparable financial loss, as well as damage to the company's reputation. From a business perspective, information security must be balanced against cost; the Gordon-Loeb Model provides a mathematical economic approach for addressing this concern.

For the individual, information security has a significant effect on privacy, which is viewed very differently in various cultures.

8

History

Since the early days of communication, diplomats and military commanders understood that it was necessary to provide some mechanism to protect the confidentiality of correspondence and to have some means of detecting tampering. Julius Caesar is credited with the invention of the Caesar cipher c. 50 B.C., which was created in order to prevent his secret messages from being read should a message fall into the wrong hands. However, for the most part protection was achieved through the application of procedural handling controls. Sensitive information was marked up to indicate that it should be protected and transported by trusted persons, guarded and stored in a secure environment or strong box. As postal services expanded, governments created official organizations to intercept, decipher, read, and reseal letters (e.g., the U.K.'s Secret Office, founded in 1653.

In the mid-nineteenth century more complex classification systems were developed to allow governments to manage their information according to the degree of sensitivity. For example, the British Government codified this, to some extent, with the publication of the Official Secrets Act in 1889. Section 1 of the law concerned espionage and unlawful disclosures of information, while Section 2 dealt with breaches of official trust. A public interest defense was soon added to defend disclosures in the interest of the state. A similar law was passed in India in 1889, The Indian Official Secrets Act, which was associated with the British colonial era and used to crack down on newspapers that opposed the Raj's policies. A newer version was passed in 1923 that extended to all matters of confidential or secret information for governance. By the time of the First World War, multi-tier classification systems were used to communicate information to and from various fronts, which

encouraged greater use of code making and breaking sections in diplomatic and military headquarters. Encoding became more sophisticated between the wars as machines were employed to scramble and unscramble information.

The establishment of computer security inaugurated the history of information security. The need for such appeared during World War II. The volume of information shared by the Allied countries during the Second World War necessitated formal alignment of classification systems and procedural controls. An arcane range of markings evolved to indicate who could handle documents (usually officers rather than enlisted troops) and where they should be stored as increasingly complex safes and storage facilities were developed. The Enigma Machine, which was employed by the Germans to encrypt the data of warfare and was successfully decrypted by Alan Turing, can be regarded as a striking example of creating and using secured information. Procedures evolved to ensure documents were destroyed properly, and it was the failure to follow these procedures which led to some of the greatest intelligence coups of the war.

9

History

Various Mainframe computers were connected online during the Cold War to complete more sophisticated tasks, in a communication process easier than mailing magnetic tapes back and forth by computer centers. As such, the Advanced Research Projects Agency (ARPA), of the United States Department of Defense, started researching the feasibility of a networked system of communication to trade information within the United States Armed Forces. In 1968, the ARPANET project was formulated by Dr. Larry Roberts, which would later evolve into what is known as the internet.

In 1973, important elements of ARPANET security were found by internet pioneer Robert Metcalfe to have many flaws such as the: "vulnerability of password structure and formats; lack of safety procedures for dial-up connections; and nonexistent user identification and authorizations", aside from the lack of controls and safeguards to keep data safe from unauthorized access. Hackers had effortless access to ARPANET, as phone numbers were known by the public. Due to these problems, coupled with the constant violation of computer security, as well as the exponential increase in the number of hosts and users of the system, "network security" was often alluded to as "network insecurity".

The end of the twentieth century and the early years of the twenty-first century saw rapid advancements in telecommunications, computing hardware and software, and data encryption. The availability of smaller, more powerful, and less expensive computing equipment made electronic data processing within the reach of small business and home users. The establishment of Transfer Control Protocol/Internetwork Protocol (TCP/IP) in the early 1980s enabled different types of computers to communicate. These computers quickly became interconnected through the internet.

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

10

Confidentiality

In information security, confidentiality "is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes." While similar to "privacy," the two

words are not interchangeable. Rather, confidentiality is a component of privacy that implements to protect our data from unauthorized viewers. Examples of confidentiality of electronic data being compromised include laptop theft, password theft, or sensitive emails being sent to the incorrect individuals.

Integrity

In IT security, data integrity means maintaining and assuring the accuracy and completeness of data over its entire lifecycle. This means that data cannot be modified in an unauthorized or undetected manner. This is not the same thing as referential integrity in databases, although it can be viewed as a special case of consistency as understood in the classic ACID model of transaction processing. Information security systems typically incorporate controls to ensure their own integrity, in particular protecting the kernel or core functions against both deliberate and accidental threats. Multi-purpose and multi-user computer systems aim to compartmentalize the data and processing such that no user or process can adversely impact another: the controls may not succeed however, as we see in incidents such as malware infections, hacks, data theft, fraud, and privacy breaches.

More broadly, integrity is an information security principle that involves human/social, process, and commercial integrity, as well as data integrity. As such it touches on aspects such as credibility, consistency, truthfulness, completeness, accuracy, timeliness, and assurance.

Availability

For any information system to serve its purpose, the information must be available when it is needed. This means the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks, such as a flood of incoming messages to the target system, essentially forcing it to shut down.

Задания закрытого типа

Задания 11-20

Выберите правильный вариант:

11. What is a firewall in computer security?
    a. A type of virus
    b. A software program
    c. A hardware device
    d. A computer network security system
12. What is the main purpose of an antivirus program?
    a. To protect a computer from viruses and other malicious software
    b. To backup data on a computer
    c. To manage passwords
    d. To monitor network traffic
13. What is a strong password?
    a. A password containing only numbers
    b. A password that is easily guessed
    c. A password containing letters, numbers and symbols
    d. A password containing only uppercase letters
14. What is a phishing attack?

a. An attack that targets vulnerabilities in a computer’s hardware
b. A type of malware
c. An attempt to steal sensitive information by pretending to be a trustworthy source
d. A type of cyberattack that targets software vulnerabilities

15. What is the purpose of encryption?
    a. To scramble data so it can only be read by the intended recipient
    b. To speed up data transfer
    c. To protect data during transit
    d. To make data more organized
16. What is two-factor authentication?
    a. A security measure that requires two forms of i5dentification before accessing a system
    b. A type of encryption
    c. A backup procedure
    d. A password manager
17. What is the purpose of a disaster recovery plan?
    a. To minimize the impact of a security breach
    b. To ensure that an organization can respond to a disaster or other emergency that affects information systems - and minimize the effect on business operations.
    c. To manage passwords
    d. To monitor network traffic
18. What is the difference between confidentiality, integrity and availability in information security?
    a. Confidentiality means keeping information private, integrity means making sure information is accurate and trustworthy, and availability means making sure information is accessible when needed.
    b. Confidentiality means making sure information is accessible when needed, integrity means keeping information private, and availability means making sure information is accurate and trustworthy.
    c. Confidentiality means making sure information is accurate and trustworthy, integrity means keeping information private, and availability means making sure information is accessible when needed.
    d. Confidentiality means making sure information is accessible when needed, integrity means making sure information is accurate and trustworthy, and availability means keeping information private.
19. What is a man-in-the-middle attack?
    a. An attack where an attacker intercepts and potentially alters communication between two parties
    b. An attack where an attacker gains unauthorized access to a system by exploiting software vulnerabilities
    c. An attack where an attacker steals sensitive information by pretending to be a trustworthy source
    d. An attack where an attacker gains access to a system by guessing a password
20. What is social engineering in the context of information security?
    a. A technique used to trick individuals into revealing information
    b. A type of software program

c. A security measure that requires two forms of identification before accessing a system
d. A hardware device used to protect a network from unauthorized access

Ответы:

11 – d
12 – a
13 – c
14 - c
15 - a
16 – a
17 – b
18 – a
19 - a
20 - a

Задания открытого типа

Задания 21 - 33

Ответьте на вопросы:

21. Speak about the challenges you can face dealing with Cloud Computing.
22. What is information?
23. Comment on the opening statement : “We live in a golden age of information”
24. What are the main sources of information?
25. What is the purpose of encryption and how does it work?
26. Explain what protection of sensitive information involves.
27. Dwell upon the role of a custodian in safeguarding information.
28. Explain the difference between information protection and information insurance.
29. What are the basic principles of information protection and information security?
30. Speak about an organization as a complex information processing system.
31. What forms does business information come in?
32. What does the value of information depend on?
33. What makes timeliness of information one of the critical factors?

Ответы:

21. The problem with cloud computing is that the user cannot view where their data is being processed or stored. And if it is not handled correctly during cloud management or implementation, risks can happen such as data theft, leaks, breaches, compromised credentials, hacked APLs, authentication breaches, account hijacking, etc.

22. Information is a fact, thought or data conveyed or described through various types of communication.

23. Information is power, it’s money and, given how much of our life is lied online, defines part of our reality.

24. There are basically two types of information sources:

- Primary information sources
- Secondary information sources

The primary information sources are those that contain the primary information that is the first hand information. Secondary information sources are those sources which are the analysis or are based on the primary information.

25. The fundamental purpose of encryption is to protect sensitive information being seen by those with unauthorized access. Encrypting communications helps you maintain data confidentiality during transmissions and storage.

26. It involves the protection of information systems and the information processed, stored and transmitted by these systems from unauthorized access, use, disclosure, disruption, modification or destruction.

27. Custodians hold stocks, bonds, and other securities on behalf of investors, preventing theft or loss. They facilitate the settlement of transactions, ensuring that ownership changes are accurately recorded and executed.

28. Information protection is just what it sounds like – protecting information through the use of Encryption, Security software and other methods designed to keep it safe. Information Assurance - on the other hand deals more with keeping the data reliable – RAID configurations, backups, non-repudiation techniques, etc.

29. The core principles of information security – confidentiality, integrity, and availability – help to protect and preserve your company's content.

30. Any organization is a complex information processing system in which actions and decisions are underpinned by an array of oral and written instructions, reports, regulations, information, and advice. Accordingly, many managers seldom look beyond the organization's boundaries in their search for information.

31. Business information comes in general surveys, data, articles, books, references, search-engines, and internal records that a business can use to guide its planning, operations, and the evaluation of its activities. Such information also comes from friends, customers, associates, and vendors.

32. It depends on it being: Up-to-date; Complete; Fit for intended use (relevant); Accurate; From a reliable source; Comprehensible Potential use of the information is an important factor in its value. The more potential uses information has the more valuable it will be.

33. Timeliness of data is one the most important aspects of database management. This refers to the availability and accessibility of data in making business decisions. Clean, well organized data dries smart decisions and makes for a better understanding of what to expect in the future.

4 СВЕДЕНИЯ О ФОНДЕ ОЦЕНОЧНЫХ СРЕДСТВ И ЕГО СОГЛАСОВАНИИ

Фонд оценочных средств для аттестации по дисциплине «Иностранный язык» представляет собой компонент основной профессиональной образовательной программы специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем

Преподаватели-разработчики – Гусева И.Г., к.ф.н, доцент; Кривко И.П., к.ф.н. доцент, Плива Е.П., к.ф.н. доцент, Пахалюк В.Г., ст. преподаватель, Рамза Н.И., ст. преподаватель.

Фонд оценочных средств рассмотрен и одобрен заведующей кафедрой иностранных языков.

Заведующая кафедрой  Г.П. Кофанова

Фонд оценочных средств рассмотрен и одобрен методической комиссией института цифровых технологий (протокол №5 от 29 августа 2024 г).

Председатель методической комиссии  О.С. Витренко