Федеральное агентство морского и речного транспорта
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Государственный университет морского и речного флота имени адмирала С.О. Макарова»

Воронежский филиал
Федерального государственного бюджетного образовательного учреждения высшего образования
«Государственный университет морского и речного флота имени адмирала С.О. Макарова»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ Б1.В.ДВ.1.2 «Перевод, аннотирование и реферирование научно-технической литературы» (английский)

(Приложение к рабочей программе дисциплины)

Уровень образования:	Высшее образование – бакалавриат	
Направление подготовки:	09.03.02 Информационные системы и технологии	
Язык обучения:	Русский	
Кафедра:	Гуманитарных и социальных наук	
Форма обучения:	Очная	Заочная
Курс:	3	4
Составитель:	Письменная В. В.	

ВОРОНЕЖ 2019 г.

СОДЕРЖАНИЕ

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ 3
1.1 Перечень компетенций и этапы их формирования в процессе 3
освоения дисциплины 3
1.2 Паспорт фонда оценочных средств для проведения текущей и промежуточной аттестации обучающихся 3
1.3 Критерии оценивания результата обучения по дисциплине и шкала оценивания 4
2. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ 5
2.1 Задания для самостоятельной работы и средства текущего контроля 5
2.2 Критерии оценки качества освоения дисциплины 13
3. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ 14
3.1 Теоретические вопросы и практические задания для проведения зачета и экзамена 14
3.2 Показатели, критерии и шкала оценивания ответов на зачете / экзамене 16

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

1.1 Перечень компетенций и этапы их формирования в процессе освоения дисциплины

В результате освоения ОПОП бакалавриата обучающийся должен овладеть следующими результатами обучения по дисциплине:

Код компетенции	Содержание компетенции	Планируемые результаты освоения дисциплины
ПК-22	способность проводить сбор, анализ научно-технической информации, отечественного и зарубежного опыта по тематике исследования	**Знать:** методы сбора и анализа научно-технической информации по тематике исследований. **Уметь:** читать и понимать аутентичные публицистические и научно-популярные тексты, используя основные виды чтения (ознакомительное, изучающее, поисковое/просмотровое) в зависимости от коммуникативной задачи; **Владеть:** навыками библиографического поиска с использованием современных информационных технологий.
ПК-26	способность оформлять полученные результаты в виде презентаций, научно-технических отчетов, статей и докладов на научно-технических конференциях	**Знать:** основную терминологию своей специальности, наиболее общеупотребительные слова и выражения; правила и этапы составления аннотации и реферата научного текста. **Уметь:** оформлять полученные результаты в виде презентаций, научно-технических отчетов, статей и докладов на научно-технических конференциях; использовать иностранный язык в в профессиональной деятельности; реферировать и аннотировать литературу по специальности. **Владеть:** навыками работы с оригинальной литературой по специальности.

1.2 Паспорт фонда оценочных средств для проведения текущей и промежуточной аттестации обучающихся

№ п/п	Контролируемые темы дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	1. 1. Перевод текста. Требования к переводу. Особенности и способы перевода терминов.	ПК-22, ПК-26	чтение и перевод текста, зачет.
	1. 2. Реферирование текста. Типы	ПК-22, ПК-26	Чтение и перевод текста, реферирование текста, зачет.

	реферата. Структура реферата. Основные этапы реферата. Специфика языка в реферате. Способы изложения информации в реферате. Наиболее общеупотребительные клише и выражения		
	1.3. Реферат-конспект	ПК-22, ПК-26	Реферирование текста, перевод текста, зачет.
	1.4. Информативный реферат	ПК-22, ПК-26	Реферирование текста, перевод текста, зачет.
	1.5. Проблемный реферат-резюме	ПК-22, ПК-26	Реферирование текста, перевод текста, зачет.
2	2.1. Аннотация. Виды аннотаций. Различия реферата и аннотации	ПК-22, ПК-26	Аннотирование текста, перевод текста, зачет.
	2.2. Общие аннотации	ПК-22, ПК-26	Аннотирование текста, перевод текста, зачет.
	2.3. Специализированные аннотации	ПК-22, ПК-26	Аннотирование текста, перевод текста, зачет.

1.3 Критерии оценивания результата обучения по дисциплине и шкала оценивания

Уровни сформированности компетенции	**Основные признаки уровня**
Пороговый (базовый) уровень **(Оценка «3», Зачтено)** (обязательный по отношению ко всем выпускникам к моменту завершения ими обучения по ОПОП)	- Общее представление о грамматических формах и конструкциях английского языка; знание основной лексики в рамках обозначенной тематики и проблематики. - Базовое умение читать и понимать аутентичные научные тексты. - Базовое владение навыками библиографического поиска литературы на иностранном языке, использование иностранного языка в профессиональной деятельности.
Повышенный (продвинутый) уровень (Оценка «4», Зачтено) (превосходит пороговый (базовый) уровень по одному или нескольким существенным признакам)	- Сформированные, но содержащие отдельные пробелы знания грамматических форм и конструкций английского языка; лексики в рамках обозначенной тематики и проблематики общения. - Сформированные, но имеющие отдельные недостатки умение читать и понимать аутентичные научные тексты, использование основных видов чтения - Сформированное, но имеющее отдельные недостатки владение навыками библиографического поиска литературы на иностранном языке,

	использование иностранного языка в профессиональной деятельности.
Высокий (превосходный) уровень (Оценка «5», Зачтено) (превосходит пороговый (базовый) уровень по всем существенным признакам, предполагает максимально возможную выраженность компетенции)	- Сформированные знания грамматических форм и конструкций английского языка; знание научной терминологии по своей специальности, овладение навыками перевода терминов и текстов по специальности. - Сформированное умение читать и понимать аутентичные научные тексты, использование основных видов чтения - Сформированные владение навыками библиографического поиска литературы на иностранном языке, использование иностранного языка в профессиональной деятельности.

2. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ

2.1 Задания для самостоятельной работы и средства текущего контроля

Раздел 1. Основы перевода и реферирования научного текста.

Тема 1. Перевод текста. Требования к переводу. Особенности и способы перевода терминов.

1) Чтение и перевод текста.

THE RISE OF IBM

IBM started in the late nineteenth century as manufacturer of electromechanical office tabulating equipment: the company took its current name in 1924. It financed one of the first digital computers, a clacking electromechanical monster known as Mark I, in 1943. IBM's first president Thomas Watson, Sr., commissioned the project, possibly as an expensive publicity stunt - research, advertising, and publicity-all came out of the same budget in those days. IBM did not immediately enter the computer business after the war and did not deliver its first computer until 1953. In 1954 IBM was only the fourth-ranked computer producer, well behind computer industry pioneer - Radio Corporation of America (RCA). That year IBM introduced the Model 650, the first computer to utilize punch-card technology.

Over the next decade, IBM made heavy investments in research and development under Thomas Watson, Jr., who took over from his father as IBM president in the mid-1950s. IBM capitalized on its manufacturing expertise to produce a full line of peripheral equipment: printers terminals, keypunch machines and card sorters that brought enormous profits for IBM and unbeatable competition for other computer manufacturers.

By the mid-1950s, IBM threatened to dominate the entire computer industry with its fast-selling Model 650. IBM also offered its computers for sale for the first time instead of renting them as it previously had insisted. This allowed leasing companies to buy computer equipment from IBM and then rent it to computer users at prices lower than IBM itself could charge. These changes opened up competition in the computer services and equipment leasing markets.

In April 1964 IBM introduced the Model 360, the first computer that came in a variety of sizes and that was compatible with many different applications. Software and peripheral devices that worked on any one of the versions also worked on the others and were also "backward compatible" with earlier IBM models. Before, users had to start over with entirely new software, printers, terminals and so on, whenever they switched to a larger computer or added a new

application. The Model 360 and its successor, the Model 370, led the company to dominance of both U.S. and international markets.

IBM's enormous success with room-sized mainframe computers eventually proved its undoing. It made unsuccessful entries into many of the specialized computer markets that later emerged. IBM abandoned the high-performance supercomputer market in the 1960s, and it entirely missed the minicomputer trend, pioneered in the early 1960s by Digital Equipment Corporation.

By the time IBM came out with its own models, minicomputers were about to be made obsolete by another new product that IBM ultimately failed to capitalize on the desktop-sized personal computer.

1. Прочитайте текст.
2. Выполните грамматический анализ каждого из предложений.
3. Найдите и переведите ключевые слова в тексте и основные термины.
4. Переведите текст, обращая внимание на грамматическую структуру оригинального текста.

Тема 2. Реферирование текста. Типы реферата. Структура реферата. Основные этапы реферата. Специфика языка в реферате. Способы изложения информации в реферате. Наиболее общеупотребительные клише и выражения

1) Реферирование и перевод текста.

A computer system

A computer system is a collection of components that work together to process data. The purpose of a computer system is to make it as easy as possible for you to use computer to solve problems. A functioning computer system combines hardware elements with software elements. The hardware elements are the mechanical devices, the system, the machinery and the electronics. The software elements are the programs written for the system. Collectively these components provide a complete computer system.

Usually, a computer system requires three basic hardware items: the central processor unit, which performs all data processing, a terminal device, which helps users to communicate with their computer system and a memory storing programs and data. These three devices are the required hardware components of any computer system. Computer system includes many other devices: a printer, a scanner and a modem. These computer devices are called hardware.

A set of instructions telling a computer what to do is a program. Programs are usually written in a Programming languages like Pascal, C++, etc. Applications are programs for specific tasks. Applications include: database software, spreadsheets calculations, word-processing on a word processor. To function hardware and software, a computer needs an operation system program. Some operation systems require users to type in commands to tell the computer what to do. Many computers use a graphical interface or point-and-click interface such as Windows.

Some interfaces allow plug-and-play, the possibility of connecting new hardware of the computer without having to adjust or configure the system to take the new hardware into account: the interface program recognizes the hardware automatically.

1. Прочитайте текст.
2. Выделите в тексте основные смысловые части.
3. Выделите в тексте ключевые слова.
4. Составьте краткий план текста.

5. Опираясь на составленный план, выполните реферирование текста.
6. Переведите текст.

Тема 1.3. Реферат-конспект.

1) Реферирование и перевод текста.

ELECTRONIC NEWSPAPERS: WILL THEY BE HERE SOON?

Economic realities are pushing the nation's dailies to the edge of a new era: delivery of written news to customers on their home screen. Confronted with a technological revolution that threatens their survival, American newspapers are joining the electronic age instead of fighting it.

Some are already experimenting with transmission of stories electronically into homes for reading on television screens. Many big newspapers are buying into cable television companies as a step toward electronic publishing. At the same time newspapers are putting more emphasis on the quality of their writing and reporting to gain new readers and keep those they already have.

Behind those developments are hard and increasingly important facts. During the 1970s total daily newspapers' circulation in the US hovered around the 60 million marks despite an 11 per cent rise in the nation's population and a 22 per cent increase in the number of households. The proportion of people who read a paper daily dropped from 69% to 57%. Afternoon newspapers would hardly compete with the television network evening program.

Growing number of publishers see electronic technology as a possible answer to these problems. They fear that if they don't go down that road the others will. The new technology is bringing all media into a common arena. The distinction that separated newspapers from magazines, that made television different from newspapers is now blurring.

Nobody knows for sure how rapidly electronic publishing will become a part of everyday journalism. Already some newspapers are leasing cable channels on which subscribers are able to read reports from various wire services, local news rewritten for viewing on a screen, weather and even advertising. Many people see a wholesale shift from print to electronics as still decades away. They cite cost factors and also argue that reading words on a screen is a much less efficient way than print to absorb large amounts of information.

For these reasons, some analysts believe electronic publishing will develop slowly, with most papers limiting themselves to transmission of stock tables, motion pictures listings, sport results, headlines, classified ads and similar materials. All these are relatively easy to read on screen and can be continuously updated.

Even such limited transmission would lead to shrinkage in the size of the daily newspaper subscribers. Therefore publishers are taking steps to make dailies more competitive with television's attractions by improving content and making new use of print technology.

1. Прочитайте текст.
2. Выделите в тексте основные смысловые части.
3. Выделите в тексте ключевые слова.
4. Составьте краткий план текста.
5. Опираясь на план, составьте реферат-конспект текста.
6. Переведите текст.

Тема 1.4. Информативный реферат.

Реферирование и перевод текста.

Data Theft: How Big a Problem?

Data theft is, quite simply, the unauthorized copying or removal of confidential information from a business or other large enterprise. It can take the form of ID-related theft or the theft of a company's proprietary information or intellectual property.

ID-related data theft occurs when customer records are stolen or illegally copied. The information stolen typically includes customers' names, addresses, phone numbers, usernames, passwords and PINs, account and credit card numbers, and, in some instances, Social Security numbers. When transmitted or sold to lower-level criminals, this information can be used to commit all manner of identity fraud. A single data theft can affect large numbers of individual victims.

Non-ID data theft occurs when an employee makes one or more copies of a company's confidential information, and then uses that information either for his own personal use or transmits that information to a competitor for the competitor's use. However it's done, this is a theft of the business' intellectual property, every bit as harmful as a theft of money or equipment. A company's confidential information includes its employee records, contracts with other firms, financial reports, marketing plans, new product specifications, and so on. Imagine you're a competitor who gets hold of a company's plans for an upcoming product launch; with knowledge beforehand, you can create your own counter-launch to blunt the impact of the other company's new product. A little inside information can be extremely valuable — and damaging for the company from which it was stolen.

Data theft can be a virtual theft (hacking into a company's systems and transmitting stolen data over the Internet) or, more often, a physical theft (stealing the data tapes or discs). In many ways, it's easier for a thief to physically steal a company's data than it is to hack into the company's network for the same purpose. Most companies give a lot of attention to Internet-based security, but less attention is typically paid to the individuals who have physical access to the same information.

One would expect data theft to be somewhat widespread. And it probably is — if we truly knew all the numbers. The problem with trying to size the data theft issue is twofold. First, many companies do not report data theft to the police or do not publicize such thefts; they're trying to avoid bad publicity. And even when data theft is reported, the dollar impact of such theft is difficult to ascertain.

Whichever number is correct, that's a lot of stolen data. Add to that the immeasurable cost of intellectual property data theft, and you get a sense of the size of the problem — it's big and it's getting bigger.

Unfortunately, there's little you as an individual can do to prevent data theft; the onus is all on the company holding the data. You could reduce your risk by limiting the number of companies with which you do business, but that may not be practical. Being alert is your only defense against this type of large-scale theft.

1. Прочитайте текст.
2. Выделите в тексте основные смысловые части.
3. Выделите в тексте ключевые слова.
4. Составьте краткий план текста.
5. Опираясь на план, составьте информативный реферат текста.
6. Переведите текст.

1. 5. Проблемный реферат-резюме.

Реферирование и перевод текста.

What is Malicious Code?

Malicious code is any code added, changed, or removed from a software system in order to intentionally cause harm or subvert the intended function of the system. Though the problem of malicious code has a long history, a number of recent, widely publicized attacks and certain economic trends suggest that malicious code is rapidly becoming a critical problem for industry, government, and individuals.

Traditional examples of malicious code include viruses, worms, Trojan Horses, and attack scripts, while more modern examples include Java attack applets and dangerous ActiveX controls. Viruses are pieces of malicious code that attach to host programs and propagate when an infected program is executed.

Worms are particular to networked computers. Instead of attaching themselves to a host program, worms carry out programmed attacks to jump from machine to machine across the network.

Trojan Horses, like viruses, hide malicious intent inside a host program that appears to do something useful (e. g., a program that captures passwords by masquerading as the login daemon.)

Attack scripts are programs written by experts that exploit security weaknesses, usually across the network, to carry out an attack. Attack scripts exploiting buffer overflows by "smashing the stack" are the most commonly encountered variety.

Java attack applets are programs embedded in Web pages that achieve foothold through a Web browser.

Dangerous ActiveX controls are program components that allow a malicious code fragment to control applications or the operating system.

Recently, the distinctions between malicious code categories have been bleeding together, and so classification has become difficult. Any computing system is susceptible to malicious code.

The growing connectivity of computers through the Internet has increased both the number of attack vectors, and the ease with which an attack can be made. More and more computers, ranging from home PCs to systems that control critical infrastructures (e. g., the power grid), are being connected to the Internet. Furthermore, people, businesses, and governments are increasingly dependent upon network-enabled communication such as e-mail or Web pages provided by information systems. Unfortunately, as these systems are connected to the Internet, they become vulnerable to attacks from distant sources. Put simply, it is no longer the case that an attacker needs physical access to a system to install or propagate malicious code.

A second trend that has enabled widespread propagation of malicious code is the size and complexity of modern information systems. Complex devices, by their very nature, introduce the risk that malicious functionality may be added (either during creation or afterwards) that extends the original device past its primary intended design. An unfortunate side effect of inherent complexity is that it until it is too late.

A third trend enabling malicious code is the degree to which systems have become extensible. From an economic standpoint, extensible systems are attractive because they provide flexible interfaces that can be adapted through new components. Unfortunately, the very nature of extensible systems makes it hard to prevent malicious code from slipping in as an unwanted extension.

1. Прочитайте текст.
2. Выделите в тексте основные смысловые части.
3. Выделите в тексте ключевые слова.
4. Составьте краткий план текста.
5. Опираясь на план, составьте проблемный реферат-резюме текста.

6. Переведите текст.

Тема 2.1. Аннотация. Виды аннотаций. Различия реферата и аннотации.

Аннотирование и перевод текста «Identification and Authentication».

Identification and Authentication.

The process of authentication is often considered to consist of two distinct phases: (1) identification and (2) (actual) authentication. Identification provides user identity to the security system. This identity is typically provided in the form of a user ID. The security system will typically search through all the abstract objects that it knows about and find the specific one for the privileges of which the actual user is currently applying. Once this is complete, the user has been identified.

Authentication is the process of validating user identity. The fact that the user claims to be represented by a specific abstract object (identified by its user ID) does not necessarily mean that this is true. To ascertain that an actual user can be mapped to a specific abstract user object in the system, and therefore be granted user rights and permissions specific to the abstract user object, the user must provide evidence to prove his identity to the system. Authentication is the process of ascertaining claimed user identity by verifying user-provided evidence.

The evidence provided by a user in the process of user authentication is called a credential. Different systems may require different types of credentials to ascertain user identity, and may even require more than one credential. In computer systems, the credential very often takes the form of a user password, which is a secret known only to the individual and the system. Credentials may take other forms, however, including PIN numbers, certificates, tickets, etc.

User identification and authentication are typically the responsibility of the operating system. Before being allowed to create even a single process on a computer, the individual must authenticate to the operating system. Applications and services may or may not honor authentication provided by the operating system, and may or may not require additional authentication upon access to them.

There are typically three components involved in the process of user authentication:

Supplicant. The party in the authentication process that will provide its identity, and evidence for it, and as a result will be authenticated. This party may also be referred to as the authenticating user, or the client.

Authenticator. The party in the authentication process that is providing resources to the client (the supplicant) and needs to ascertain user identity to authorize and audit user access to resources. The authenticator can also be referred to as the server.

Security authority/database. A storage or mechanism to check user credentials. This can be as simple as a flat file, or a server on the network providing for centralized user authentication, or a set of distributed authentication servers that provide for user authentication within the enterprise or on the Internet.

In a simple scenario, the supplicant, authenticator, and security database may reside on the same computer. It is also possible and somewhat common for network applications to have the supplicant on one computer and the authenticator and security database collocated on another computer. It is also possible to have the three components geographically distributed on multiple computers. It is important to understand that the three parties can communicate independently with one another. Depending on the authentication mechanism used, some of the communication channels might not be used — at least not by an actual dialogue over the network. The type of communication and whether or not it is used depends on the authentication mechanism and the model of trust that it implements.

1. Прочитайте текст.

2. Выделите в тексте основные смысловые части.
3. Выделите в тексте ключевые слова.
4. Составьте краткий план текста.
5. Опираясь на план, составьте аннотацию текста.
6. Переведите текст.

2.2. Общие аннотации.

Аннотирование текста и перевод текста.

Understanding Denial of Service

A denial-of-service attack is different in goal, form, and effect than most of the attacks that are launched at networks and computers. Most attackers involved in cybercrime seek to break into a system, extract its secrets, or fool it into providing a service that they should not be allowed to use. Attackers commonly try to steal credit card numbers or proprietary information, gain control of machines to install their software or save their data, deface Web pages, or alter important content on victim machines. Frequently, compromised machines are valued by attackers as resources that can be turned to whatever purpose they currently deem important.

In DDoS attacks, breaking into a large number of computers and gaining malicious control of them is just the first step. The attacker then moves on to the DoS attack itself, which has a different goal—to prevent victim machines or networks from offering service to their legitimate users. No data is stolen, nothing is altered on the victim machines, and no unauthorized access occurs. The victim simply stops offering service to normal clients because it is preoccupied with handling the attack traffic. While no unauthorized access to the victim of the DDoS flood occurs, a large number of other hosts have previously been compromised and controlled by the attacker, who uses them as attack weapons. In most cases, this is unauthorized access, by the legal definition of that term.

While the denial-of-service effect on the victim may sound relatively benign, especially when one considers that it usually lasts only as long as the attack is active, for many network users it can be devastating. Use of Internet services has become an important part of our daily lives. Following are some examples of the damaging effects of DoS attacks.

• Sites that offer services to users through online orders make money only when users can access those services. For example, a large book-selling site cannot sell books to its customers if they cannot browse the site's Web pages and order products online. A DoS attack on such sites means a severe loss of revenue for as long as the attack lasts. Prolonged or frequent attacks also inflict long-lasting damage to a site's reputation — customers who were unable to access the desired service are likely to take their business to the competition. Sites whose reputations were damaged may have trouble attracting new customers or investor funding in the future.

• Large news sites and search engines are paid by marketers to present their advertisements to the public. The revenue depends on the number of users that view the site's Web page. A DoS attack on such a site means a direct loss of revenue from the marketers, and may have the long-lasting effect of driving the customers to more easily accessible sites. Loss of popularity translates to a direct loss of advertisers' business.

• Numerous businesses have come to depend on the Internet for critical daily activities. A DoS attack may interrupt an important videoconference meeting or a large customer order.

• The Internet is increasingly being used to facilitate management of public services, such as water, power, and sewage, and to deliver critical information for important activities, such as weather and traffic reports for docking ships. A DoS attack that disrupts these critical services will directly affect even people whose activities are not related to computers or the Internet. It may even endanger human lives.

• A vast number of people use the Internet on a daily basis for entertainment or for communicating with friends and family. While a DoS attack that disrupts these activities may not cause them any serious damage, it is certainly an unpleasant experience that they wish to avoid. If such disruptions occur frequently, people are likely to stop using the Internet for these purposes, in favor of more reliable technologies.

1. Прочитайте текст.
2. Выделите в тексте основные смысловые части.
3. Выделите в тексте ключевые слова.
4. Составьте краткий план текста.
5. Опираясь на план, составьте общую аннотацию текста.
6. Переведите текст.

2.3. Специализированные аннотации.

Аннотирование и перевод текста.

"Phishing" is a new term widely popularized in mainstream media in the second half of 2003. Microsoft defines it as any type of attack that attempts to lure users to a fake Web site to enter in sensitive information that is then used for identity and banking theft. This
normally occurs via an e-mail, directing users to a phishing Web site.

Originally, phishers obtained passwords by tricking users into supplying the passwords in response to an e-mail request. Although this method is still prevalent today, with firms such as the major banks, eBay, and PayPal being among the largest targets, more complex and creative methods have been developed to attempt to fool the end user.

These include such methods as directing users to fake Web sites that appear as if they are issued by the same company (i. e., eBay, Chase, U.S. Bank), man-in-the-middle proxies to capture data, Trojan-horse keyloggers, and screen captures. Phishing activity has been increasing dramatically over the past few years.

The United States leads as the country hosting the most phishing sites, with 24.27 per cent. The other top countries are China (17.23 per cent), Republic of Korea (11 per cent), and Canada, with 4.05 per cent.

These statistics point out that this is a growing activity and increasingly used as a criminal activity to open an account, make an unauthorized transaction, obtain log-in credentials, or perform some other kind of identity theft.

A First Data survey in 2005 revealed that over 60 per cent of online users had inadvertently visited a spoofed site. A Consumer Reports survey indicated that 30 per cent of users had reduced their overall use of the Internet and 25 per cent had discontinued online shopping. Where once there was trust in the major brands, as indicated earlier, this trust is eroding with respect to online transactions, in large part due to a lack of trust in Web sites and fear of identity theft.

Educating consumers about the dangers of phishing is a delicate balance. On the one hand, consumers need to be vigilant in not responding to e-mails with links to sites requesting their personal information; on the other hand, consumers should not be afraid to participate in online commerce and use e-mail wisely. Phishing has become so prevalent that the Federal Trade Commission (FTC) issued a consumer alert advising consumers how not to get hooked by a phishing scam. The key points from the FTC included the following.

• If you get an e-mail or pop-up message that asks for personal or financial information, do not reply. And do not click on the link in the message, either.
• Area codes can mislead (and may not be in your area due to Voice-over-IP technology).
• Use antivirus and antispyware software, as well as a firewall, and update them all.
• Do not e-mail personal or financial information.

• Review credit card and bank account statements as soon as you receive them.
• Be cautious about opening any attachment or downloading any file from e-mails.
• Forward spam that is phishing for information to spam@uce.gov and to the bank or company that was impersonated with the e-mail. If you believe you have been scammed, file a complaint at www.ftc.gov.

However, the entire burden cannot be on the consumer. There are multiple known delivery methods, attack vectors, and solutions to help minimize the risk. Organizations must be vigilant in their education of internal and external customers, the design of secure software, the maintenance of appropriate patch levels, and providing a phishing reporting and remediation capability and must remain continuously aware of the techniques and threats related to this type of attack.

1. Прочитайте текст.
2. Выделите в тексте основные смысловые части.
3. Выделите в тексте ключевые слова.
4. Составьте краткий план текста.
5. Опираясь на план, составьте специализированную аннотацию текста.
6. Переведите текст.

2.2 Критерии оценки качества освоения дисциплины

Качество освоения дисциплины оценивается по степени успешности ответов на прктических занятиях, качества выполнения самостоятельной работы и результатов прохождения тестирования.

Критерии оценивания реферирования и аннотирования текста.

Оценка ***«Отлично»*** ставится, если учащийся полностью понял текст, полно и точно передаёт содержание текста, высказывание логично, использованы средства логической связи, использованы разнообразные лексические и грамматические конструкции в соответствии с поставленной задачей и требованиям данного года обучения языку. Грамматические ошибки либо отсутствуют, либо не препятствуют решению коммуникативной задачи. Наличие выводов и заключения

Оценка «***Хорошо***» ставится, если учащийся полностью понял текст, полно и точно передаёт содержание текста, высказывание логично, использованы средства логической связи, использованы разнообразные лексические и грамматические конструкции в соответствии с поставленной задачей и требованиям программы обучения. Допущены незначительные грамматические или лексические ошибки, которые не препятствуют решению коммуникативной задачи. Наличие выводов и заключения.

Оценка «***Удовлетворительно***» ставится, если учащийся понял основную тему текста, содержание текста передано частично или нарушена логичность высказывания. Допущено умеренное количество лексических и грамматических ошибок. Коммуникативная задача решена, но выводы и заключение отсутствуют.

Оценка «***Неудовлетворительно***» ставится, если учащийся неверно понял основную тему текста. Высказывание нелогично. Допущено большое количество лексических и грамматических ошибок. Коммуникативная задача не решена.

Критерии перевода текста

Оценка **«*Отлично*»** ставится, если перевод текста полностью соответствует содержанию оригинального текста, т.е. текста на иностранном языке. Переведен и сам текст, и

заголовок. Понятна направленность текста и общее его содержание В переводе текста нет (или допущены 1-2) лексических ошибок. Правильно переведены все общеупотребительные простые слова, фразеологические обороты, устойчивые словосочетания. Верно передан смысл сложных слов. Все профессиональные термины переведены верно. В переводе отсутствуют грамматические ошибки (орфографические, пунктуационные и др.) Все грамматические конструкции, обороты, придаточные предложения, переведены правильно Перевод полностью соответствует профессиональной стилистике и направленности текста. Перевод высказывания логичный, последовательный, сохранена структура оригинального текста, текст разделен на абзацы

Оценка «***Хорошо***» ставится, если Переведен и сам текст, и заголовок. Понятна направленность текста и общее его содержание. В переводе текста нет (или допущены 1-2) лексических ошибок. Отдельные слова соответствуют общей тематике текста. Смысл текста передан. Неточно переведены некоторые общеупотребительные слова, устойчивые словосочетания, сложные слова, фразеологические обороты. Профессиональные термины в основном переведены верно. В переводе отсутствуют грамматические ошибки (орфографические, пунктуационные и др.) Некоторые грамматические конструкции, обороты, придаточные предложения, переведены правильно Перевод в основном соответствует профессиональной стилистике и направленности текста. Перевод высказывания не везде логичный, последовательный, но сохранена структура оригинального текста, текст разделен на абзацы.

Оценка «***Удовлетворительно***» ставится, если перевод текста на 60 % от общего объема соответствует содержанию оригинального текста, т.е. текста на иностранном языке. Переведен и сам текст, и заголовок. Понятна направленность текста и общее его содержание В переводе текста 1-2 лексические ошибки, но общая тематика текста понятна. Смысл текста передан. Неправильно переведены некоторые общеупотребительные слова, устойчивые словосочетания, сложные слова, фразеологические обороты. Профессиональные термины в основном переведены верно, но 3-4 термина могут иметь неточный перевод В переводе 3-4 грамматические ошибки (орфографические, пунктуационные и др.) Большая часть грамматических конструкции, обороты, придаточные предложения, переведены неправильно. Перевод в основном, соответствует профессиональной стилистике и направленности текста. Перевод высказывания не везде логичный, последовательный, не сохранена структура оригинального текста, текст не разделен на абзацы

Оценка «***Неудовлетворительно***» ставится, если учащийся не понял смысла задания. Заголовок текста и текст переведен, но перевод текста не соответствует его основному содержанию. Смысл текста не понятен. Содержание перевода лишь на 10 % от общего объема текста (и менее) отражает текст.

3. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

3.1 Теоретические вопросы и практические задания для проведения зачета и экзамена

Вопросы для подготовки к зачету

Теоретические вопросы для подготовки к зачету

1. Требования к переводу. Особенность и способы перевода терминов

2. Особенности реферирование текста. Типы реферата.
3. Структура реферата. Основные этапы реферата.
4. Специфика языка в реферате. Способы изложения информации в реферате.
5. Особенности составления реферата-конспекта.
6. Особенности составления информативного реферата.
7. Особенности составления проблемного реферата-резюме.
8. Аннотация. Виды аннотаций.
9. Основные различия реферата и аннотации.
10. Особенности составления общей аннотации.
11. Особенности составления специализированной аннотации.

Практические вопросы к зачету

Задание 1 к тексту:
1. Выполните реферат-конспект
2. Выполните реферат-резюме
3. Выполните информативный реферат
4. Составьте общую аннотацию текста
5. Составьте специализированную аннотацию текста

Текст.

Information Warfare: Its Application in Military and Civilian Contexts

The lexicon of information warfare (IW), or cyberwar, to use a common variant, has been around for more than two decades, but for most of that time it has remained the preserve of the defense community. The privileging of military thinking is myopic. Information warfare concepts deserve to be liberated from their military associations and introduced into other discourse communities concerned with understanding the social consequences of pervasive computing. Already, the principles and practices of information warfare are being exhibited, more or less wittingly, in a variety of civilian contexts, and there are good grounds for assuming that this trend will intensify, causing potentially serious social problems and creating novel challenges for the criminal justice system. To paraphrase a well-worn cliché, information warfare is too important to be left to the military.

The term “information warfare” is still popularly associated with high-technology weapons and broadcast images of Cruise missiles seeking out Iraqi or other military targets with apparently unerring accuracy. The media’s early focus on smart bombs and intelligent battle systems masked the potentially deeper societal implications of virtual warfare strategies. That, however, is beginning to change, as journalists and pundits foreground computer hacking and data corruption as pivotal information warfare techniques. Simplifications and confusions notwithstanding, an axial assumption of information age warfare is that brains matter more than brawn. In tomorrow’s battlefield, be it military or civilian, information technology will act as a force multiplier. Traditional notions about the bases of superiority existing between attacker and target may thus require redefinition.

Pandemic access to digital networks creates a downward adjustment of established power differentials at all levels of society.

The principles and practice of information warfare have potentially much wider implications for society at large in a networked age. We consider four spheres of activity in which information warfare may very soon become relatively commonplace: military, corporate/economic, community/social, and personal.

3.2 Показатели, критерии и шкала оценивания ответов на зачете / экзамене

Зачет	
Оценка «зачтено»	**Оценка «не зачтено»**
Студент показывает знание основного учебного материала в объеме, необходимом для продожения обучения. Справляется с выполнением практических заданий, предусмотренных программой, существующие погрешности не существенны и не препятствуют решению коммуникативной задачи	Ответ студента обнаруживает существенные пробелы в знании основного учебного материала, ответ носит отрывочный, поверхностный характер, студент не справляется с выполнением практических заданий, предусмотренных программой обучения, допускает существенные грамматические и лексические ошибки; коммуникативная задача не решена