

Федеральное государственное бюджетное образовательное учреждение высшего образования «Тамбовский государственный университет имени Г.Р. Державина»
Институт математики, физики и информационных технологий
Кафедра математического моделирования и информационных технологий

УТВЕРЖДАЮ:
Директор института



Н. Л. Королева
«05» июля 2021 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине Б1.В.ДВ.04.3 Теоретические основы защиты информации на
английском языке

Направление подготовки/специальность: 10.03.01 - Информационная безопасность

Профиль/направленность/специализация: Безопасность компьютерных систем

Уровень высшего образования: бакалавриат

Квалификация: Бакалавр

год набора: 2021

Автор программы:

Кандидат педагогических наук, доцент Михайлова Елена Михайловна

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.03.01 - Информационная безопасность (уровень бакалавриата) (приказ Министерства образования и науки РФ от «17» ноября 2020 г. № 1427).

Рабочая программа принята на заседании Кафедры математического моделирования и информационных технологий «18» мая 2021 г. Протокол № 9

Рассмотрена и одобрена на заседании Ученого совета Института математики, физики и информационных технологий, Протокол от «05» июля 2021 г. № 5.

СОДЕРЖАНИЕ

1. Цели и задачи дисциплины.....	4
2. Место дисциплины в структуре ОП бакалавра.....	5
3. Объем и содержание дисциплины.....	5
4. Контроль знаний обучающихся и типовые оценочные средства.....	17
5. Методические указания для обучающихся по освоению дисциплины (модуля).....	29
6. Учебно-методическое и информационное обеспечение дисциплины.....	31
7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы.....	31

1. Цели и задачи дисциплины

1.1 Цель дисциплины – формирование компетенций:

ПК-3 Способен администрировать средства защиты информации прикладного и системного программного обеспечения

1.2 Типы задач профессиональной деятельности, к которым готовятся обучающиеся в рамках освоения дисциплины:

- организационно-управленческий

1.3 Дисциплина ориентирована на подготовку обучающихся к профессиональной деятельности в сфере: 06 Связь, информационные и коммуникационные технологии (в сфере техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере)

1.4 В результате освоения дисциплины у обучающихся должны быть сформированы:

Обобщенные трудовые функции / трудовые функции / трудовые или профессиональные действия (при наличии профстандарта)	Код и наименование компетенции ФГОС ВО, необходимой для формирования трудового или профессионального действия	Индикаторы достижения компетенций
	ПК-3 Способен администрировать средства защиты информации прикладного и системного программного обеспечения	На основе современных технологий обеспечений информационной безопасности администрирует средства защиты информации прикладного и системного программного обеспечения для обеспечения безопасности программ и данных

1.5 Согласование междисциплинарных связей дисциплин, обеспечивающих освоение компетенций:

ПК-3 Способен администрировать средства защиты информации прикладного и системного программного обеспечения

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Форма обучения			
		Очная (семестр)			
		2	6	7	8
1	Защита программ и данных			+	
2	Избранные вопросы информационной безопасности		+	+	
3	Преддипломная практика				+
4	Современные технологии обеспечения информационной безопасности	+			
5	Теоретические основы защиты информации	+			

2. Место дисциплины в структуре ОП бакалавриата:

Дисциплина «Теоретические основы защиты информации на английском языке» относится к части, формируемой участниками образовательных отношений, учебного плана ОП по направлению подготовки 10.03.01 - Информационная безопасность.

Дисциплина «Теоретические основы защиты информации на английском языке» изучается в 2 семестре.

3. Объем и содержание дисциплины

3.1. Объем дисциплины:

Вид учебной работы	Очная (всего часов)
Общая трудоёмкость дисциплины	72
Контактная работа	48
Лекции (Лекции)	16
Лабораторные (Лаб. раб.)	32
Самостоятельная работа (СР)	24
Зачет	-

3.2. Содержание курса:

№ темы	Название раздела/темы	Вид учебной работы, час.			Формы текущего контроля
		Лек ции	Лаб · раб.	СР	
		О	О	О	
2 семестр					
1	Основные понятия теории информационной безопасности.	2	4	3	Тестирование
2	Информация как объект защиты.	2	4	3	Тестирование
3	Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности.	2	4	3	Опрос
4	Угрозы информационной безопасности.	2	4	3	Тестирование
5	Построение систем защиты от угрозы нарушения конфиденциальнос ти .	2	4	3	Тестирование

6	Построение систем защиты от угрозы нарушения целостности информации и отказа доступа.	2	3	3	Тестирование
7	Политика и модели безопасности.	2	3	2	Тестирование
8	Обзор международных стандартов информационной безопасности.	1	3	2	Выполнение практических заданий
9	Информационные войны и информационное противоборство.	1	3	2	Выполнение практических заданий

Тема 1. Основные понятия теории информационной безопасности. (ПК-3)

Лекция.

The subject area of the theory of information security. Systematization of concepts in the field of information security. Basic terms and definitions of legal concepts in the field of information relations and information protection. Concepts of the subject area "Information protection". Basic principles of building protection systems. The concept of comprehensive information protection. Tasks of information protection. Means of implementing comprehensive information protection.

Лабораторные работы.

1. The information is:
 - a) information received from the media;
 - b) only documented information about persons, objects, facts, events;
 - c) information about persons, objects, facts, events, phenomena and processes, regardless of the form of their presentation;
 - d) only information contained in electronic databases.
2. Information
 - a) does not disappear when consumed;
 - b) becomes available if it is contained on a tangible medium;
 - c) is subject only to "moral wear and tear";
 - d) is characterized by all the listed properties.
3. The information recorded on a material carrier, with the details that allow it to be identified, is called:
 - a) reliable;
 - b) confidential;
 - c) documented;
 - d) a trade secret.
4. The information and telecommunication network is:
 - a) a technological system designed to transmit information over communication lines, access to which is carried out using computer technology;
 - b) a technological system designed for transmission over the Internet, which is accessed using computer technology;
 - c) a technological system designed to transmit information over a local network, which is accessed using computer technology.
5. Access to information is:
 - a) the possibility of obtaining information;

- b) the possibility of obtaining information and using it;
 - c) the possibility of obtaining information and its dissemination.
6. Providing information is an action aimed at:
- a) to receive information from a certain circle of persons;
 - b) to receive information by the manager and transfer information to a certain circle of persons;
 - c) to receive information from a certain circle of persons or to transmit information to a certain circle of persons.
7. Information security is:
- a) protection of information and supporting infrastructure from accidental or intentional impacts of a natural or accidental nature that may cause unacceptable damage to subjects of information relations, including owners and users of information and supporting infrastructure;
 - b) the security of the company's software products from accidental or intentional impacts of a natural or accidental nature;
 - c) the security of information circulating on the network from accidental or intentional impacts of a natural or accidental nature.
8. Information security is the security of information:
- a) from disclosure, distortion, loss;
 - b) from disclosure, distortion, loss or reduction of the degree of accessibility of information, as well as its illegal replication;
 - c) from transfer to third parties, distortion and illegal use.
9. The threat is:
- a) the potential to violate information security in a certain way;
 - b) a system of software language organizational and technical means designed for the accumulation and collective use of data;
 - c) the determination process meets the current state of development requirements of this stage.
10. Effective information security is possible:
- a) only on the basis of the integrated use of all known methods and approaches to solving this problem;
 - d) only when using certified information security tools;
 - e) only when using technical means of information protection;
 - f) All answers are correct.

Задания для самостоятельной работы.

- Show the connection between the level of development of society and information security technologies.
- In what directions is the theory of information security currently developing?
- What is the contribution of Russian scientists to the theory of information security?
- What is the reason for the increased interest in the problems of information security?
- What are the differences between formal and informal approaches to the problems of information security?
- What, in your opinion, are the main difficulties of ensuring information security at the present time?
- What is an information system? Telecommunications system? An automated system?
- What are the legal concepts in the field of information protection?
- What is information protection? Information security?
- Describe the concepts related to the organization of information protection.
- What are the basic principles of building information security systems?
- What is an integrated approach to information security?
- What are the main tasks of information protection?
- Prove that the above set of protection functions is complete.
- What is the relationship between the various means of information protection? Are there any priority ones among them?
- What are the main means of implementing a comprehensive information security system?
- What are moral and ethical means of information protection?

Prove the need for a combination of different means of information protection. 20. Give examples of formal and informal means of protection?

What are information security centers and what is their role in the development of the theory and practice of information security?

Тема 2. Информация как объект защиты. (ПК-3)

Лекция.

The concept of information as an object of protection. Levels of information presentation. The main properties of the protected information. Types and forms of information presentation. Information resources. Structure and scale of information value. Classification of information resources. The legal regime of information resources.

Лабораторные работы.

1. Documents and arrays of documents in information systems (libraries, archives, funds, data banks, depositories, museum repositories, etc.):

- a) information resources;
- b) information products;
- c) information perspectives.

2. Information resources are one of the types of social and economic resources:

- a) business factors;
- b) factors of production;
- c) factors of activity.

3. The level of development of the information services sector largely determines the degree of proximity to such a society:

- a) information;
- b) open;
- c) closed.

4. Document flow is:

- a) the movement of documents in the organization from the moment of their creation or receipt to the completion of execution or dispatch; +
- b) type of state, municipal, scientific, commercial and non-commercial activity;
- c) it is a system of standards for information, library and publishing.

5. Authentication is:

- a) a mechanism for delimiting access to data and system functions;
- b) the ability to verify the identity of the user; +
- c) search and research of mathematical methods of information transformation.

6. In information systems, documented information is presented in the form of:

- a) files, folders, arrays, databases, programs;
- b) databases and software;
- c) files and databases.

7. Information resources can be:

- a) open, closed;
- b) open and restricted access;
- c) restricted access.

8. The information protection mode is set:

- a) in relation to information classified as a state secret;
- b) with respect to confidential information;
- c) in relation to information classified as a state secret and personal data.

9. What is subject to mandatory certification:

- a) automated systems of public authorities that process documented information with limited access, as well as means of protecting these systems;

- b) automated systems of municipal authorities that process documented information with limited access, as well as means of protecting these systems;
- c) automated systems that process information constituting a state secret.

Задания для самостоятельной работы.

1. What is information and what are the levels of its presentation?
2. List the main media, features of their use and protection.
3. What properties determine the value of information?
4. What criteria for evaluating the value of information can you offer?
5. Give examples of the different dependence of the value of information on time.
6. What is meant by information resources?
7. What is not allowed to be classified as restricted access information?
8. What is meant by confidential information?
9. What kinds of secrets are there?
10. What is the purpose of the list of confidential information of the enterprise?

Тема 3. Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности. (ПК-3)

Лекция.

Information security and its place in the national security system of the Russian Federation. Information security and information protection bodies, their functions and tasks, regulatory activities.

Лабораторные работы.

1. What are the functions of the heads of enterprises in the organization of information protection?
2. What are the main functions of the FSTEC?
3. What are the main functions of the FSB?
4. What are the main functions of the interdepartmental commission?
5. What are the main functions of the Security Council of the Russian Federation?
6. Who is responsible for the use of non-certified information security tools in automated systems?

Задания для самостоятельной работы.

1. What is the place of information security in the national security system of the Russian Federation?
2. Formulate the main provisions of the Information Security Doctrine of the Russian Federation.
3. What are the main objectives of information protection?
4. What are the main tasks in the field of information security?
5. What is the structure of the state information protection system?
6. Who is responsible for violating the data protection regime?
7. Show the role of various ministries and departments in the protection of information.

Тема 4. Угрозы информационной безопасности. (ПК-3)

Лекция.

Vulnerability analysis of the system. Classification of information security threats. The main directions and methods of threat implementation. Informal model of the violator. Vulnerability assessment of the system.

Лабораторные работы.

1. When designing a protection system, it is necessary:
 - a) determining the list of threats and building a model of the violator;
 - b) definition of software and hardware means of information protection;
 - c) identification of certified means of protection and construction of a model of the violator.
2. Vulnerability analysis is a mandatory procedure
 - a) when analyzing information security tools;
 - b) when certifying the object of informatization;
 - c) when determining the model of the violator.

3. Natural threats to information security are caused by:

- a) human activities;
- b) errors in the design of ASOI, its elements or software development;
- c) the effects of objective physical processes or natural phenomena independent of man;
- d) the selfish aspirations of intruders;
- e) errors in the actions of personnel.

4. Artificial threats to information security caused by:

- a) human activities;
- b) errors in the design of ASOI, its elements or software development;
- c) the effects of objective physical processes or natural phenomena independent of man;
- d) the selfish aspirations of intruders;
- e) errors in the actions of personnel.

5. The main unintended artificial threats of ASOI include:

- a) physical destruction of the system by explosion, arson, etc.;
- b) interception of side electromagnetic, acoustic and other radiation devices and communication lines;
- c) changing the operating modes of devices or programs, strike, sabotage of personnel, setting powerful active interference, etc.;
- d) reading residual information from RAM and from external storage devices;
- e) unintentional actions leading to partial or complete system failure or destruction of hardware, software, information resources of the system.

6. Outsiders who violate information security include:

- a) representatives of organizations interacting on issues of ensuring the life of the organization;
- b) technical equipment maintenance personnel;
- c) technical staff servicing the building;
- d) users;
- e) security personnel.
- f) representatives of competing organizations.
- g) persons who violated the access regime;

7. Which category is the most risky for the company in terms of possible fraud and security breaches?

- a) employees;
- b) hackers;
- c) attackers;
- d) contractors (persons working under the contract).

8. Who is ultimately responsible for ensuring that data is classified and protected?

- a) data owners;
- b) users;
- c) administrators;
- d) the manual.

Задания для самостоятельной работы.

1. Using the example of several different threats, show that their implementation will lead to a change in one of the main properties of the protected information (confidentiality, integrity, accessibility).
2. Give examples of systems for which the greatest security threat is a violation of the confidentiality of information.
3. For which systems (give examples) is the most dangerous violation of the integrity of information?
4. In which systems is the availability of information in the first place?
5. What is the difference between the concepts of "violation of confidentiality of information", "unauthorized access to information", "information leakage"?
6. Determine the list of the main threats to the AU, consisting of an autonomous computer without access to the network, located in one of the laboratories of the university.

7. Build an informal intruder model for a training computer lab.
8. Output the formula for calculating the strength of the three-level protective shell.
9. Describe the protective shells and the list of barriers used in the educational computer laboratory

Тема 5. Построение систем защиты от угрозы нарушения конфиденциальности . (ПК-3)

Лекция.

Definition and main methods of unauthorized access. Methods of protection against NSD. Organizational methods of protection against NSD. Engineering and technical methods of protection against NSD. Construction of protection systems against the threat of leakage through technical channels. Identification and authentication. The main directions and purposes of using cryptographic methods. Protection against the threat of violation of confidentiality at the level of information content.

Лабораторные работы.

1. The main sources of threats to information security:
 - a) Theft of hard drives, network connection, insider trading;
 - b) Data interception, data theft, system architecture change;+
 - c) Data theft, bribery of system administrators, violation of work regulations.
2. Determine the types of information security:
 - a) Personal, corporate, state;
 - b) Client, server, network;
 - c) Local, global, mixed.
3. Note the bulk of information security threats:
 - a) Trojan programs ;
 - b) Spyware;
 - c) Worms.
4. The type of identification and authentication that has become most widespread:
 - a) PKI systems;
 - b) permanent passwords;
 - c) one-time passwords.
5. Determine under which systems the spread of viruses occurs most dynamically:
 - a) Windows;
 - b) Mac OS;
 - c) Android.
6. Information security objectives - timely detection, warning:
 - a) unauthorized access, exposure to the network;
 - b) impacts on the network;
 - c) emergency situations.
7. Identify the main objects of information security:
 - a) Computer networks, databases;
 - b) Information systems, psychological state of users;
 - c) Business-oriented, commercial systems.
8. Methods of protection against NSD:
 - a) organizational, legal, technological;
 - b) moral and ethical, financial;
 - c) engineering, technical, legal.
9. In accordance with GOST R 50922-96, three types of information leakage are considered. The main causes of information leakage are:
 - a) errors in the design of the system and protection systems, non-compliance by personnel with norms, requirements, operating rules;
 - b) the conduct of technical and intelligence intelligence by the opposing side;

c) the use of non-certified protective equipment, personnel errors.

10. In accordance with GOST R 50922-96, three types of information leakage are considered:

- a) disclosure;
- b) unauthorized access to information;
- c) obtaining protected information by intelligence services;
- d) Theft, modification, disclosure.

11. Effective protection against NSD is possible when combined

- a) organizational, legal methods;
- b) certified means of protection, organizational methods.
- c) technical, regulatory and legal methods;

12. To block the channels of unauthorized access to information, it is of great importance:

- a) building identification and authentication systems;
- b) building identification systems;
- c) application of technical, regulatory and legal methods.

13. Cryptographic methods of protecting information from unauthorized access are the only reliable means of protection when transmitting information via:

- a) communication channels;
- b) over the Internet;
- c) over the corporate network.

Задания для самостоятельной работы.

1. What is the difference between the terms "NSD" and "Violation of confidentiality of information"?
2. What is meant by information leakage?
3. How are information leakage channels classified?
4. How should I choose measures to protect the confidentiality of information?
5. Define user identification and authentication. What is the difference between these concepts?
6. List the main authentication methods. Which one, in your opinion, is the most effective?
7. What are the main access control methods used in information systems known to you? What are their advantages and disadvantages?
8. Why is password authentication currently considered unreliable?
9. What are the authentication methods using items of a given type? Name those that have become widespread recently.
10. Define the cipher and formulate the basic requirements for it.
11. Explain what is meant by a perfect cipher.
12. . Why can most modern cryptograms be uniquely decrypted?
13. How does the state regulate the use of cryptographic protection tools?

Тема 6. Построение систем защиты от угрозы нарушения целостности информации и отказа доступа. (ПК-3)

Лекция.

Protecting the integrity of information during storage. Protection of information integrity during processing . Protecting the integrity of information during transportation. Protection against the threat of violation of the integrity of information at the content level. Building protection systems against the threat of denial of access to information. Protection of semantic analysis and relevance of information. Application of general scientific methods, laws of physics, mathematical apparatus, methods of modeling and forecasting in the field of information security.

Лабораторные работы.

1. What is the name of intentionally distorted information?
 - a) Misinformation
 - b) Informative flow
 - c) Reliable information

- d) Ceases to be information
2. What is the name of the information to which access is restricted?
 - a) Unavailable
 - b) Illegal
 - c) Open
 - d) Confidential
3. What ways can information be obtained?
 - a) Conducting, purchasing and illegally obtaining scientific research information
 - b) The seizure and hacking of PC information of scientific research
 - c) Obtaining information from external sources and scrambling research information
 - d) The seizure and hacking of a security system for scientific research information
4. What are the names of computer systems in which information security is ensured?
 - a) Protected CS
 - b) Unsafe CS
 - c) Self-sufficient CS
 - d) Self-regulating COP
5. The main document on the basis of which the information security policy is carried out?
 - a) Political information security
 - b) Information security Regulations
 - c) Information Security Program
 - d) Protectorate
6. Depending on the form of presentation, the information can be divided into?
 - a) Thought, word and speech
 - b) Speech, documented and telecommunication
 - c) Digital, audio and secret
 - d) Digital, audio
7. What processes include the processes of collecting, processing, accumulating, storing, searching and distributing information
 - a) Information processes
 - b) Thought processes
 - c) Machine processes
 - d) Microprocessors
8. What is called information protection?
 - a) Name activities to prevent unintended impacts on protected information
 - b) They call activities to prevent leakage of protected information
 - c) They call activities to prevent unauthorized impacts on protected information
 - d) All answers are correct
9. By unintentional impact on protected information is understood?
 - a) The possibility of its transformation, in which the content of the information is changed to false information;
 - b) The process of its transformation, in which the content of the information is changed to false;
 - c) The impact on it due to user errors, failure of technical or software tools and the impact of natural phenomena;
 - d) Not restricting access to certain sectors of the economy or to specific industries.
10. Encryption of information is:
 - a) The process of its transformation, in which the content of information becomes incomprehensible to non-authorized entities
 - b) The process of transformation, in which information is deleted
 - c) The process of its transformation, in which the content of the information is changed to false

d) The process of converting information into machine code

Задания для самостоятельной работы.

1. What are the ways to control the integrity of the message flow?
2. What are the ways to control the integrity of messages with mutual trust of the parties?
3. How to control the integrity of messages with a high level of interference in communication channels?
4. How is the exchange of digitally signed documents organized?
5. What is the difference and similarity between conventional and digital signatures?
6. What principles should be followed to preserve the integrity of data during their processing?
7. Why are data integrity control issues related to information security issues?
8. What does data integrity control mean at the content level? Give examples.
9. How to ensure data integrity during storage?
10. What is reliability and what is the difference between hardware reliability and software reliability?
11. Should we distinguish between protection from accidental threats and from the actions of an attacker while ensuring unhindered access to information? Justify your answer.
12. How to protect the software from studying the logic of its operation?
13. Suggest measures to ensure more reliable operation of the university LAN.
14. How does the reliability of the equipment change over time?
15. What are the ways to improve the reliability of equipment and communication lines?

Тема 7. Политика и модели безопасности. (ПК-3)

Лекция.

Security policy. Subject-object models of access differentiation. Axioms of security policy. Discretionary access policies and models. Password access control systems. Policy and models of mandatory access. Information-theoretical models. Policies and models of thematic access differentiation. Role-based security model.

Лабораторные работы.

- 1) With an authorized security policy, a set of labels with the same values forms:
 - a) An area of equal criticality;
 - (b) The area of equal access;
 - c) Security level;
 - d) Availability level.
- 2) The degree of protection of information from negative impact on it in terms of violation of its physical and logical integrity or unauthorized use is:
 - a) vulnerability of information;
 - b) reliability of information;
 - c) information security;
 - d) information security.
- 3) Verification of the authenticity of the subject by the identifier presented by him to make a decision on granting him access to the resources of the system is:
 - a) authorization;
 - b) audit;
 - c) identification;
 - d) authentication.
- 4) Using the private key information:
 - a) copied;
 - b) broadcast;
 - c) stands for;
 - d) encrypted.
- 5) The set of properties that determine the suitability of information to meet certain needs in accordance with its purpose is called:

- a) the relevance of information;
 - b) availability;
 - c) the quality of information;
 - d) integrity.
- 6) The disadvantage of the security policy end-state model is:
- a) changing the communication line;
 - b) static;
 - c) complexity of implementation;
 - d) low degree of reliability.
- 7) The access control method, in which each object of the system is assigned a criticality label that determines the value of information, is called:
- a) identifiable;
 - b) mandatory;
 - c) selective;
 - d) privileged.
- 8) Organizational requirements for the protection system:
- a) management and identification;
 - b) administrative and hardware;
 - (c) Administrative and procedural;
 - d) hardware and physical.
- 9) The basis of the security policy is:
- a) software;
 - b) risk management;
 - c) access management method;
 - d) selection of the communication channel.
- 10) The science studying mathematical methods of information protection by its transformation is:
- a) cryptography;
 - b) shorthand;
 - c) cryptanalysis;
 - d) cryptology.
- 11) According to the Orange Book, a group of criteria has minimal protection:
- a) C;
 - b) A;
 - c) B;
 - d) D.
- 12) From the point of view of the SCC, the main task of security means is to ensure:
- a) the safety of information;
 - b) protection against NSD;
 - c) ease of implementation;
 - d) reliability of operation.
- 13) According to the Orange Book, a group of criteria has discretionary protection:
- a) D;
 - b) A;
 - c) B;
 - d) C.
- 14) With a qualitative approach, the risk is measured in terms of:
- a) monetary losses;
 - b) set using the ranking scale;
 - (c) Expert assessments;

d) the amount of information.

15) According to the "European Criteria", a formal description of security functions is required at the level:

- a) E5;
- b) E7;
- c) E4;
- d) E6.

Задания для самостоятельной работы.

1. Preparation for practical classes, repetition of the study of lecture material;
2. Preparation for lectures, repetition of the educational material of previous lectures;
3. Study of the materials of the lecture course on the tasks for independent study issued by the teacher in the classroom;

Тема 8. Обзор международных стандартов информационной безопасности. (ПК-3)

Лекция.

The role of information security standards. Criteria for the security of computer systems of the US Department of Defense (Orange Book), TCSEC. European Information Technology Security Criteria (ITSEC). Federal criteria for the security of information technology in the USA. Unified information technology security criteria. Group of international standards 270000.

Лабораторные работы.

The purpose of the work: familiarization with the main international standards regulating the protection of confidential information.

When performing the task, it is necessary to analyze the content of the following main international safety standards:

1. International Information Security Management Standard ISO 17799.
1. General information technology security criteria GOST ISO/IEC 15408.
2. Criteria for assessing the reliability of computer systems ("Orange Book").
3. Canadian criteria and General Criteria.
4. COBIT standard ("Control objects for information and related technologies").

It is necessary to compare these standards with the Russian regulatory framework in the field of information security and assess their applicability in Russia.

Задания для самостоятельной работы.

1. Preparation for practical classes, repetition of the study of lecture material.
2. Preparation for lectures, repetition of the educational material of previous lectures.
3. Study of the materials of the lecture course on the tasks for independent study issued by the teacher in the classroom.

Тема 9. Информационные войны и информационное противоборство. (ПК-3)

Лекция.

Definition and main types of information wars. The requirements are divided into three groups: strategy, accountability, guarantees. Information technology warfare. Information and psychological warfare.

Лабораторные работы.

Practical task.

The purpose of the work:

1. To consolidate knowledge of the regulatory and legislative framework of the Russian Federation on the issues of information warfare.
2. To consolidate the concepts: information operations, psychological operations, operational camouflage, electronic warfare.

Tasks:

Option No. 1.

1. What are the social and personal prerequisites for the emergence of information operations and wars?

2. What are the features of strategic planning in information wars?
3. Describe the basic strategies of information wars.
4. Describe the strategies used by the opposition to overthrow the government in the process of "color" revolutions.
5. Humanitarian aspects of information weapons and illustrate them with the actual examples found from your life or from the life of modern society.

Option #2.

1. The true goals and reasons for the use of information weapons.
2. Means and methods of information and psychological warfare.
3. Types of threats to the security of the individual, society and the state in the context of information and psychological warfare.
4. Sources of threats to the security of the individual, society and the state in the context of information and psychological warfare.
5. Describe the features of rapid response to suddenly identified actions (events) of informational and psychological aggression (war).

Задания для самостоятельной работы.

1. Preparation for practical classes, repetition of the study of lecture material;
2. Preparation for lectures, repetition of the educational material of previous lectures;
3. Study of the materials of the lecture course on the tasks for independent study issued by the teacher in the classroom;

4. Контроль знаний обучающихся и типовые оценочные средства

4.1. Распределение баллов:

2 семестр

- посещаемость – 20 баллов
- текущий контроль – 60 баллов
- контрольные срезы – 2 среза по 10 баллов каждый
- премиальные баллы – 20 баллов

Распределение баллов по заданиям:

№ те мы	Название темы / вид учебной работы	Формы текущего контроля / срезы	Мах. кол-во баллов	Методика проведения занятия и оценки
1.	Основные понятия теории информационной безопасности.	Тестирование	8	Тест состоит из вопросов с выбором ответа. 8 баллов - студент правильно отвечает более чем на 90% вопросов. 4-6 баллов – студент правильно отвечает на 50-80% вопросов в тесте. 2-3 балла - студент правильно отвечает на 30-50% вопросов. 1 балл - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
2.	Информация как объект защиты.	Тестирование(контрольный срез)	10	Тест состоит из вопросов с выбором ответа. 10 баллов - студент правильно отвечает более чем на 90% вопросов. 4-6 баллов – студент правильно отвечает на 50-80% вопросов в тесте. 2-3 балла - студент правильно отвечает на 30-50% вопросов. 1 балл - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.

3.	Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности.	Опрос	9	<p>Опрос предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Все члены группы могут участвовать в обсуждении, добавлять информацию, дискутировать, задавать вопросы и т.д.</p> <p>Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения поставленной учебной задачи; - своевременность и эффективность использования наглядных пособий и технических средств при ответе; - использование дополнительного материала; - рациональность использования времени, отведенного на задание. <p>9 баллов – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы</p> <p>5 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>2 балла – студент владеет теоретическим материалом по теме практического занятия, иногда затрудняется при ответе на вопросы, не умеет сформулировать свою точку зрения на обсуждаемую проблему</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается.</p>
4.	Угрозы информационной безопасности.	Тестирование	9	<p>Тест состоит из вопросов с выбором ответа.</p> <p>9 баллов - студент правильно отвечает более чем на 90% вопросов.</p> <p>4-6 баллов – студент правильно отвечает на 50-80% вопросов в тесте.</p> <p>2-3 балла - студент правильно отвечает на 30-50% вопросов.</p> <p>1 балл - студент правильно отвечает на 25-30% вопросов в тесте.</p> <p>Менее 25% правильных ответов баллов не дает.</p>
5.	Построение систем защиты от угрозы нарушения конфиденциальности .	Тестирование	9	<p>Тест состоит из вопросов с выбором ответа.</p> <p>9 баллов - студент правильно отвечает более чем на 90% вопросов.</p> <p>4-6 баллов – студент правильно отвечает на 50-80% вопросов в тесте.</p> <p>2-3 балла - студент правильно отвечает на 30-50% вопросов.</p> <p>1 балл - студент правильно отвечает на 25-30% вопросов в тесте.</p> <p>Менее 25% правильных ответов баллов не дает.</p>
6.	Построение систем защиты от угрозы нарушения целостности информации и отказа доступа.	Тестирование	9	<p>Тест состоит из вопросов с выбором ответа.</p> <p>9 баллов - студент правильно отвечает более чем на 90% вопросов.</p> <p>4-6 баллов – студент правильно отвечает на 50-80% вопросов в тесте.</p> <p>2-3 балла - студент правильно отвечает на 30-50% вопросов.</p> <p>1 балл - студент правильно отвечает на 25-30% вопросов в тесте.</p> <p>Менее 25% правильных ответов баллов не дает.</p>

7.	Политика и модели безопасности.	Тестирование(контрольный срез)	10	Тест состоит из вопросов с выбором ответа. 10 баллов - студент правильно отвечает более чем на 90% вопросов. 4-6 баллов – студент правильно отвечает на 50-80% вопросов в тесте. 2-3 балла - студент правильно отвечает на 30-50% вопросов. 1 балл - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
8.	Обзор международных стандартов информационной безопасности.	Выполнение практических заданий	8	Лабораторные работы выполняются по тематике практических занятий. 8 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию 5 баллов – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы 2 балла - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы
9.	Информационные войны и информационное противоборство.	Выполнение практических заданий	8	Лабораторные работы выполняются по тематике практических занятий. 8 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию 5 баллов – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы 2 балла - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы
10.	Посещаемость		20	20 баллов – стопроцентное посещение занятий студентом 10 баллов – посещаемость студента составляет не менее 80 % занятий 5 баллов – посещаемость студента составляет не менее 50 % занятий 3 балла – посещаемость студента составляет не менее 25 % занятий
11.	Премиальные баллы		20	Дополнительные премиальные баллы могут быть начислены: - за проект, выполненный по заказу работодателя и реализованный на практике – 20 баллов; - постоянная активность во время практических занятий – 10 баллов; - полностью подготовленная к публикации статья по тематике в рамках дисциплины – 10 баллов; - участие с докладом во всероссийской олимпиаде по тематике изучаемой дисциплины – 20 баллов; - участие в выставке по тематике изучаемой дисциплины – 20 баллов; - публикация статьи по тематике изучаемой дисциплины в сборнике студенческих работ / материалах всероссийской конференции / журнале из перечня ВАК – 10 / 15 / 20

12.	Индивидуальные задания, с помощью которых можно набрать дополнительные баллы	20	Решение кейса (10 баллов) Прохождение тестирования (30 вопросов) по всему курсу дисциплины (10 баллов)
13.	Итого за семестр	100	

Итоговая оценка по зачету выставляется в 100-балльной шкале и в традиционной четырехбалльной шкале. Перевод 100-балльной рейтинговой оценки по дисциплине в традиционную четырехбалльную осуществляется следующим образом:

100-балльная система	Традиционная система
50 - 100 баллов	Зачтено
0 - 49 баллов	Не зачтено

4.2 Типовые оценочные средства текущего контроля

Выполнение практических заданий

Тема 8. Обзор международных стандартов информационной безопасности.

The purpose of the work: familiarization with the main international standards regulating the protection of confidential information.

When performing the task, it is necessary to analyze the content of the following main international safety standards:

1. International Information Security Management Standard ISO 17799.
1. General information technology security criteria GOST ISO/IEC 15408.
2. Criteria for assessing the reliability of computer systems ("Orange Book").
3. Canadian criteria and General Criteria.
4. COBIT standard ("Control objects for information and related technologies").

It is necessary to compare these standards with the Russian regulatory framework in the field of information security and assess their applicability in Russia.

Тема 9. Информационные войны и информационное противоборство.

Practical task.

The purpose of the work:

1. To consolidate knowledge of the regulatory and legislative framework of the Russian Federation on the issues of information warfare.
2. To consolidate the concepts: information operations, psychological operations, operational camouflage, electronic warfare.

Tasks:

Option No. 1.

1. What are the social and personal prerequisites for the emergence of information operations and wars?
2. What are the features of strategic planning in information wars?
3. Describe the basic strategies of information wars.
4. Describe the strategies used by the opposition to overthrow the government in the process of "color" revolutions.
5. Humanitarian aspects of information weapons and illustrate them with the actual examples found from your life or from the life of modern society.

Option #2.

1. The true goals and reasons for the use of information weapons.
2. Means and methods of information and psychological warfare.

3. Types of threats to the security of the individual, society and the state in the context of information and psychological warfare.
4. Sources of threats to the security of the individual, society and the state in the context of information and psychological warfare.
5. Describe the features of rapid response to suddenly identified actions (events) of informational and psychological aggression (war).

Опрос

Тема 3. Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности.

1. What are the functions of the heads of enterprises in the organization of information protection?
2. What are the main functions of the FSTEC?
3. What are the main functions of the FSB?
4. What are the main functions of the interdepartmental commission?
5. What are the main functions of the Security Council of the Russian Federation?
6. Who is responsible for the use of non-certified information security tools in automated systems?

Тестирование

Тема 1. Основные понятия теории информационной безопасности.

1. The information is:
 - a) information received from the media;
 - b) only documented information about persons, objects, facts, events;
 - c) information about persons, objects, facts, events, phenomena and processes, regardless of the form of their presentation;
 - d) only information contained in electronic databases.
2. Information
 - a) does not disappear when consumed;
 - b) becomes available if it is contained on a tangible medium;
 - c) is subject only to "moral wear and tear";
 - d) is characterized by all the listed properties.
3. The information recorded on a material carrier, with the details that allow it to be identified, is called:
 - a) reliable;
 - b) confidential;
 - c) documented;
 - d) a trade secret.
4. The information and telecommunication network is:
 - a) a technological system designed to transmit information over communication lines, access to which is carried out using computer technology;
 - b) a technological system designed for transmission over the Internet, which is accessed using computer technology;
 - c) a technological system designed to transmit information over a local network, which is accessed using computer technology.
5. Access to information is:
 - a) the possibility of obtaining information;
 - b) the possibility of obtaining information and using it;
 - c) the possibility of obtaining information and its dissemination.
6. Providing information is an action aimed at:
 - a) to receive information from a certain circle of persons;

- b) to receive information by the manager and transfer information to a certain circle of persons;
- c) to receive information from a certain circle of persons or to transmit information to a certain circle of persons.

7. Information security is:

- a) protection of information and supporting infrastructure from accidental or intentional impacts of a natural or accidental nature that may cause unacceptable damage to subjects of information relations, including owners and users of information and supporting infrastructure;
- b) the security of the company's software products from accidental or intentional impacts of a natural or accidental nature;
- c) the security of information circulating on the network from accidental or intentional impacts of a natural or accidental nature.

8. Information security is the security of information:

- a) from disclosure, distortion, loss;
- b) from disclosure, distortion, loss or reduction of the degree of accessibility of information, as well as its illegal replication;
- c) from transfer to third parties, distortion and illegal use.

9. The threat is:

- a) the potential to violate information security in a certain way;
- b) a system of software language organizational and technical means designed for the accumulation and collective use of data;
- c) the determination process meets the current state of development requirements of this stage.

10. Effective information security is possible:

- a) only on the basis of the integrated use of all known methods and approaches to solving this problem;
- d) only when using certified information security tools;
- e) only when using technical means of information protection;
- f) All answers are correct.

Тема 2. Информация как объект защиты.

1. Documents and arrays of documents in information systems (libraries, archives, funds, data banks, depositories, museum repositories, etc.):

- a) information resources;
- b) information products;
- c) information perspectives.

2. Information resources are one of the types of social and economic resources:

- a) business factors;
- b) factors of production;
- c) factors of activity.

3. The level of development of the information services sector largely determines the degree of proximity to such a society:

- a) information;
- b) open;
- c) closed.

4. Document flow is:

- a) the movement of documents in the organization from the moment of their creation or receipt to the completion of execution or dispatch; +
- b) type of state, municipal, scientific, commercial and non-commercial activity;
- c) it is a system of standards for information, library and publishing.

5. Authentication is:

- a) a mechanism for delimiting access to data and system functions;
- b) the ability to verify the identity of the user; +

- c) search and research of mathematical methods of information transformation.
- 6. In information systems, documented information is presented in the form of:
 - a) files, folders, arrays, databases, programs;
 - b) databases and software;
 - c) files and databases.
- 7. Information resources can be:
 - a) open, closed;
 - b) open and restricted access;
 - c) restricted access.
- 8. The information protection mode is set:
 - a) in relation to information classified as a state secret;
 - b) with respect to confidential information;
 - c) in relation to information classified as a state secret and personal data.
- 9. What is subject to mandatory certification:
 - a) automated systems of public authorities that process documented information with limited access, as well as means of protecting these systems;
 - b) automated systems of municipal authorities that process documented information with limited access, as well as means of protecting these systems;
 - c) automated systems that process information constituting a state secret.

Тема 4. Угрозы информационной безопасности.

- 1. When designing a protection system, it is necessary:
 - a) determining the list of threats and building a model of the violator;
 - b) definition of software and hardware means of information protection;
 - c) identification of certified means of protection and construction of a model of the violator.
- 2. Vulnerability analysis is a mandatory procedure
 - a) when analyzing information security tools;
 - b) when certifying the object of informatization;
 - c) when determining the model of the violator.
- 3. Natural threats to information security are caused by:
 - a) human activities;
 - b) errors in the design of ASOI, its elements or software development;
 - c) the effects of objective physical processes or natural phenomena independent of man;
 - d) the selfish aspirations of intruders;
 - e) errors in the actions of personnel.
- 4. Artificial threats to information security caused by:
 - a) human activities;
 - b) errors in the design of ASOI, its elements or software development;
 - c) the effects of objective physical processes or natural phenomena independent of man;
 - d) the selfish aspirations of intruders;
 - e) errors in the actions of personnel.
- 5. The main unintended artificial threats of ASOI include:
 - a) physical destruction of the system by explosion, arson, etc.;
 - b) interception of side electromagnetic, acoustic and other radiation devices and communication lines;
 - c) changing the operating modes of devices or programs, strike, sabotage of personnel, setting powerful active interference, etc.;
 - d) reading residual information from RAM and from external storage devices;
 - e) unintentional actions leading to partial or complete system failure or destruction of hardware, software, information resources of the system.

6. Outsiders who violate information security include:

- a) representatives of organizations interacting on issues of ensuring the life of the organization;
- b) technical equipment maintenance personnel;
- c) technical staff servicing the building;
- d) users;
- e) security personnel.
- f) representatives of competing organizations.
- g) persons who violated the access regime;

7. Which category is the most risky for the company in terms of possible fraud and security breaches?

- a) employees;
- b) hackers;
- c) attackers;
- d) contractors (persons working under the contract).

8. Who is ultimately responsible for ensuring that data is classified and protected?

- a) data owners;
- b) users;
- c) administrators;
- d) the manual.

Тема 5. Построение систем защиты от угрозы нарушения конфиденциальности .

1. The main sources of threats to information security:

- a) Theft of hard drives, network connection, insider trading;
- b) Data interception, data theft, system architecture change;+
- c) Data theft, bribery of system administrators, violation of work regulations.

2. Determine the types of information security:

- a) Personal, corporate, state;
- b) Client, server, network;
- c) Local, global, mixed.

3. Note the bulk of information security threats:

- a) Trojan programs ;
- b) Spyware;
- c) Worms.

4. The type of identification and authentication that has become most widespread:

- a) PKI systems;
- b) permanent passwords;
- c) one-time passwords.

5. Determine under which systems the spread of viruses occurs most dynamically:

- a) Windows;
- b) Mac OS;
- c) Android.

6. Information security objectives - timely detection, warning:

- a) unauthorized access, exposure to the network;
- b) impacts on the network;
- c) emergency situations.

7. Identify the main objects of information security:

- a) Computer networks, databases;
- b) Information systems, psychological state of users;
- c) Business-oriented, commercial systems.

8. Methods of protection against NSD:

a) organizational, legal, technological;

b) moral and ethical, financial;

c) engineering, technical, legal.

9. In accordance with GOST R 50922-96, three types of information leakage are considered. The main causes of information leakage are:

a) errors in the design of the system and protection systems, non-compliance by personnel with norms, requirements, operating rules;

b) the conduct of technical and intelligence intelligence by the opposing side;

c) the use of non-certified protective equipment, personnel errors.

10. In accordance with GOST R 50922-96, three types of information leakage are considered:

a) disclosure;

b) unauthorized access to information;

c) obtaining protected information by intelligence services;

d) Theft, modification, disclosure.

11. Effective protection against NSD is possible when combined

a) organizational, legal methods;

b) certified means of protection, organizational methods.

c) technical, regulatory and legal methods;

12. To block the channels of unauthorized access to information, it is of great importance:

a) building identification and authentication systems;

b) building identification systems;

c) application of technical, regulatory and legal methods.

13. Cryptographic methods of protecting information from unauthorized access are the only reliable means of protection when transmitting information via:

a) communication channels;

b) over the Internet;

c) over the corporate network.

Тема 6. Построение систем защиты от угрозы нарушения целостности информации и отказа доступа.

1. What is the name of intentionally distorted information?

a) Misinformation

b) Informative flow

c) Reliable information

d) Ceases to be information

2. What is the name of the information to which access is restricted?

a) Unavailable

b) Illegal

c) Open

d) Confidential

3. What ways can information be obtained?

a) Conducting, purchasing and illegally obtaining scientific research information

b) The seizure and hacking of PC information of scientific research

c) Obtaining information from external sources and scrambling research information

d) The seizure and hacking of a security system for scientific research information

4. What are the names of computer systems in which information security is ensured?

a) Protected CS

b) Unsafe CS

c) Self-sufficient CS

d) Self-regulating COP

5. The main document on the basis of which the information security policy is carried out?
 - a) Political information security
 - b) Information security Regulations
 - c) Information Security Program
 - d) Protectorate
6. Depending on the form of presentation, the information can be divided into?
 - a) Thought, word and speech
 - b) Speech, documented and telecommunication
 - c) Digital, audio and secret
 - d) Digital, audio
7. What processes include the processes of collecting, processing, accumulating, storing, searching and distributing information
 - a) Information processes
 - b) Thought processes
 - c) Machine processes
 - d) Microprocessors
8. What is called information protection?
 - a) Name activities to prevent unintended impacts on protected information
 - b) They call activities to prevent leakage of protected information
 - c) They call activities to prevent unauthorized impacts on protected information
 - d) All answers are correct
9. By unintentional impact on protected information is understood?
 - a) The possibility of its transformation, in which the content of the information is changed to false information;
 - b) The process of its transformation, in which the content of the information is changed to false;
 - c) The impact on it due to user errors, failure of technical or software tools and the impact of natural phenomena;
 - d) Not restricting access to certain sectors of the economy or to specific industries.
10. Encryption of information is:
 - a) The process of its transformation, in which the content of information becomes incomprehensible to non-authorized entities
 - b) The process of transformation, in which information is deleted
 - c) The process of its transformation, in which the content of the information is changed to false
 - d) The process of converting information into machine code

Тема 7. Политика и модели безопасности.

- 1) With an authorized security policy, a set of labels with the same values forms:
 - a) An area of equal criticality;
 - (b) The area of equal access;
 - c) Security level;
 - d) Availability level.
- 2) The degree of protection of information from negative impact on it in terms of violation of its physical and logical integrity or unauthorized use is:
 - a) vulnerability of information;
 - b) reliability of information;
 - c) information security;
 - d) information security.
- 3) Verification of the authenticity of the subject by the identifier presented by him to make a decision on granting him access to the resources of the system is:

- a) authorization;
 - b) audit;
 - c) identification;
 - d) authentication.
- 4) Using the private key information:
- a) copied;
 - b) broadcast;
 - c) stands for;
 - d) encrypted.
- 5) The set of properties that determine the suitability of information to meet certain needs in accordance with its purpose is called:
- a) the relevance of information;
 - b) availability;
 - c) the quality of information;
 - d) integrity.
- 6) The disadvantage of the security policy end-state model is:
- a) changing the communication line;
 - b) static;
 - c) complexity of implementation;
 - d) low degree of reliability.
- 7) The access control method, in which each object of the system is assigned a criticality label that determines the value of information, is called:
- a) identifiable;
 - b) mandatory;
 - c) selective;
 - d) privileged.
- 8) Organizational requirements for the protection system:
- a) management and identification;
 - b) administrative and hardware;
 - c) Administrative and procedural;
 - d) hardware and physical.
- 9) The basis of the security policy is:
- a) software;
 - b) risk management;
 - c) access management method;
 - d) selection of the communication channel.
- 10) The science studying mathematical methods of information protection by its transformation is:
- a) cryptography;
 - b) shorthand;
 - c) cryptanalysis;
 - d) cryptology.
- 11) According to the Orange Book, a group of criteria has minimal protection:
- a) C;
 - b) A;
 - c) B;
 - d) D.
- 12) From the point of view of the SCC, the main task of security means is to ensure:
- a) the safety of information;
 - b) protection against NSD;

- c) ease of implementation;
- d) reliability of operation.

13) According to the Orange Book, a group of criteria has discretionary protection:

- a) D;
- b) A;
- c) B;
- d) C.

14) With a qualitative approach, the risk is measured in terms of:

- a) monetary losses;
- b) set using the ranking scale;
- (c) Expert assessments;
- d) the amount of information.

15) According to the "European Criteria", a formal description of security functions is required at the level:

- a) E5;
- b) E7;
- c) E4;
- d) E6.

4.3 Промежуточная аттестация по дисциплине проводится в форме зачета

Типовые вопросы зачета (ПК-3)

1. Теория защиты информации. Основные направления
2. Виды угроз. Основные нарушения.
3. Общая модель воздействия на информацию.
4. Общая модель процесса нарушения физической целостности информации.
5. Методы определения требований к защите информации.
6. Допущения в моделях оценки уязвимости информации.
7. Классификация требований к средствам защиты информации.
8. Способы и средства защиты информации.
9. Способы «абсолютной системы защиты».

Типовые задания для зачета (ПК-3)

1. Содержание интересов личности, общества и государства в информационной сфере.
2. Источники и содержание угроз в информационной сфере.
3. Классы информационных ресурсов.
4. Общая схема обеспечения информационной безопасности
5. Ретроспективный анализ развития подходов к защите информации.
6. Сущность и содержание эмпирического, концептуально-эмпирического теоретико-концептуального подходов к защите информации

4.4. Шкала оценивания промежуточной аттестации

Оценка	Компетенции	Дескрипторы (уровни) – основные признаки освоения (показатели достижения результата)
--------	-------------	--

«зачтено» (50 - 100 баллов)	ПК-3	Демонстрирует высокий уровень теоретических знаний методологического базиса решения задач защиты информации. Анализирует существующие методики определений требования к защите информации. Превосходно владеет знанием принципов обеспечения защиты информации. Способен продемонстрировать современные подходы к администрированию средств защиты информации прикладного и системного программного обеспечения.
«не зачтено» (0 - 49 баллов)	ПК-3	Не способен продемонстрировать знания методологического базиса решения задач защиты информации. Не анализирует существующие методики определений требования к защите информации. Не владеет знанием принципов обеспечения защиты информации. Не способен продемонстрировать современные подходы к администрированию средств защиты информации прикладного и системного программного обеспечения.

5. Методические указания для обучающихся по освоению дисциплины (модуля)

5.1 Методические указания по организации самостоятельной работы обучающихся:

Приступая к изучению дисциплины, в первую очередь обучающимся необходимо ознакомиться содержанием рабочей программы дисциплины (РПД), которая определяет содержание, объем, а также порядок изучения и преподавания учебной дисциплины, ее раздела, части.

Для самостоятельной работы важное значение имеют разделы «Объем и содержание дисциплины», «Учебно-методическое и информационное обеспечение дисциплины» и «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы».

В разделе «Объем и содержание дисциплины» указываются все разделы и темы изучаемой дисциплины, а также виды занятий и планируемый объем в академических часах.

В разделе «Учебно-методическое и информационное обеспечение дисциплины» указана рекомендуемая основная и дополнительная литература.

В разделе «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы» содержится перечень профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины.

5.2 Рекомендации обучающимся по работе с теоретическими материалами по дисциплине

При изучении и проработке теоретического материала необходимо:

- просмотреть еще раз презентацию лекции в системе MOODLe, повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной дополнительной литературы;
- при самостоятельном изучении теоретической темы сделать конспект, используя рекомендованные в РПД источники, профессиональные базы данных и информационные справочные системы;
- ответить на вопросы для самостоятельной работы, по теме представленные в пункте 3.2 РПД.
- при подготовке к текущему контролю использовать материалы фонда оценочных средств (ФОС).

5.3 Рекомендации по работе с научной и учебной литературой

Работа с основной и дополнительной литературой является главной формой самостоятельной работы и необходима при подготовке к устному опросу на семинарских занятиях, к дебатам, тестированию, экзамену. Она включает проработку лекционного материала и рекомендованных источников и литературы по тематике лекций.

Конспект лекции должен содержать реферативную запись основных вопросов лекции, в том числе с опорой на размещенные в системе MOODLe презентации, основных источников и литературы по темам, выводы по каждому вопросу. Конспект может быть выполнен в рамках распечатки выдачи презентаций лекций или в отдельной тетради по предмету. Он должен быть аккуратным, хорошо читаемым, не содержать не относящуюся к теме информацию или рисунки.

Конспекты научной литературы при самостоятельной подготовке к занятиям должны содержать ответы на каждый поставленный в теме вопрос, иметь ссылку на источник информации с обязательным указанием автора, названия и года издания используемой научной литературы. Конспект может быть опорным (содержать лишь основные ключевые позиции), но при этом позволяющим дать полный ответ по вопросу, может быть подробным. Объем конспекта определяется самим студентом.

В процессе работы с основной и дополнительной литературой студент может:

- делать записи по ходу чтения в виде простого или развернутого плана (создавать перечень основных вопросов, рассмотренных в источнике);
- составлять тезисы (цитирование наиболее важных мест статьи или монографии, короткое изложение основных мыслей автора);
- готовить аннотации (краткое обобщение основных вопросов работы);
- создавать конспекты (развернутые тезисы).

5.4. Рекомендации по подготовке к отдельным заданиям текущего контроля

Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Все члены группы могут участвовать в обсуждении, добавлять информацию, дискутировать, задавать вопросы и т.д.

Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:

- правильность ответа по содержанию;
- полнота и глубина ответа;
- сознательность ответа;
- логика изложения материала;
- рациональность использованных приемов и способов решения поставленной учебной задачи;
- своевременность и эффективность использования наглядных пособий и технических средств при ответе;
- использование дополнительного материала;
- рациональность использования времени, отведенного на задание.

Устный опрос может сопровождаться презентацией, которая подготавливается по одному из вопросов практического занятия. При выступлении с презентацией необходимо обращать внимание на такие моменты как:

- содержание презентации: актуальность темы, полнота ее раскрытия, смысловое содержание, соответствие заявленной темы содержанию, соответствие методическим требованиям (цели, ссылки на ресурсы, соответствие содержания и литературы), практическая направленность, соответствие содержания заявленной форме, адекватность использования технических средств учебным задачам, последовательность и логичность презентуемого материала;
- оформление презентации: объем (оптимальное количество), дизайн (читаемость, наличие и соответствие графики и анимации, звуковое оформление, структурирование информации, соответствие заявленным требованиям), оригинальность оформления, эстетика, использование возможности программной среды, соответствие стандартам оформления;
- личностные качества: ораторские способности, соблюдение регламента, эмоциональность, умение ответить на вопросы, систематизированные, глубокие и полные знания по всем разделам программы;

- содержание выступления: логичность изложения материала, раскрытие темы, доступность изложения, эффективность применения средств ИКТ, способы и условия достижения результативности и эффективности для выполнения задач своей профессиональной или учебной деятельности, доказательность принимаемых решений, умение аргументировать свои заключения, выводы.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная литература:

1. Передков В.М., Митрошкин А.Г. Информационная безопасность и защита информации. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)
2. Лопатин Д.В., Калинина Ю.В. Безопасные информационные технологии : электрон. учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)
3. Тамб гос. ун-т им. Г.Р. Державина, Ин-т математики, физики и информатики Техническая защита информации : учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)

6.2 Дополнительная литература:

1. Загинайлов Ю. Н. Основы информационной безопасности: курс визуальных лекций : учебное пособие. - Москва|Берлин: Директ-Медиа, 2015. - 105 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=362895>
2. Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие. - Москва|Берлин: Директ-Медиа, 2015. - 253 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=276557>
3. Аверченков В. И., Рытов М. Ю., Кувыклин А. В., Рудановский М. В. Аудит информационной безопасности органов исполнительной власти : учебное пособие. - 4-е изд., стер.. - Москва: Флинта, 2016. - 100 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=93259>
4. Комплексное обеспечение информационной безопасности автоматизированных систем : лабораторный практикум. - Ставрополь: Северо-Кавказский Федеральный университет (СКФУ), 2016. - 242 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=458012>
5. Петренко В. И. Теоретические основы защиты информации : учебное пособие. - Ставрополь: Северо-Кавказский Федеральный университет (СКФУ), 2015. - 222 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=458204>

6.3 Иные источники:

1. Курс «Стандарты информационной безопасности» - <https://www.intuit.ru/studies/courses/30/30/info>
2. Курс «Основы информационной безопасности» - <https://www.intuit.ru/studies/courses/10/10/info>

7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы

Для проведения занятий по дисциплине необходимо следующее материально-техническое обеспечение: учебные аудитории для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещения для самостоятельной работы.

Учебные аудитории и помещения для самостоятельной работы укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы укомплектованы компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета.

Для проведения занятий лекционного типа используются наборы демонстрационного оборудования, обеспечивающие тематические иллюстрации (проектор, ноутбук, экран/ интерактивная доска).

Лицензионное и свободно распространяемое программное обеспечение:

Microsoft Windows 10

Google Chrome

Microsoft Office Профессиональный плюс 2007

Профессиональные базы данных и информационные справочные системы:

1. Электронный каталог Фундаментальной библиотеки ТГУ. – URL: <http://biblio.tsutmb.ru/elektronnyij-katalog>
2. Университетская библиотека онлайн: электронно-библиотечная система. – URL: <https://biblioclub.ru>
3. Консультант студента. Гуманитарные науки: электронно-библиотечная система. – URL: <https://www.studentlibrary.ru>
4. Научная электронная библиотека eLIBRARY.ru. – URL: <https://elibrary.ru>
5. Научная электронная библиотека Российской академии естествознания. – URL: <https://www.monographies.ru>
6. Российская государственная библиотека. – URL: <https://www.rsl.ru>
7. Российская национальная библиотека. – URL: <http://nlr.ru>
8. Президентская библиотека имени Б.Н. Ельцина. – URL: <https://www.prilib.ru>
9. Электронная библиотека РФФИ. – URL: <https://www.rfbr.ru/rffi/ru/library>

Электронная информационно-образовательная среда

https://auth.tsutmb.ru/authorize?response_type=code&client_id=moodle&state=xyz

Взаимодействие преподавателя и студента в процессе обучения осуществляется посредством мультимедийных, гипертекстовых, сетевых, телекоммуникационных технологий, используемых в электронной информационно-образовательной среде университета.