МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Северо-Кавказский филиал
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

Утверждаю
Зам. директора по УР
_____ Н.А. Андреева
«28» _____04_____ 2026 г.

Основы информационной безопасности Б1.О.24

рабочая программа дисциплины

Кафедра **Информационная безопасность**
Направление подготовки **11.03.02 Инфокоммуникационные технологии и системы связи**
Профиль **Защищенные инфокоммуникационные системы**
Формы обучения **очная, заочная**

Распределение часов дисциплины по семестрам (для очной формы обучения), курсам (для заочной формы обучения)

Вид учебной работы	ОФ		ЗФ	
	4 года		5 лет	
	ЗЕ	часов	ЗЕ	часов
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	2	72/5	2	72/2, 3
Контактная работа, в том числе (по семестрам, курсам):		32/5		2/2, 10/3
Лекции		16/5		2/2, 4/3
Лабораторных работ				
Практических занятий		16/5		6/3
Семинаров				
Самостоятельная работа		40/5		34/2, 26/3
Контроль				
Число контрольных работ (по курсам)				
Число КР (по семестрам, курсам)				
Число КП (по семестрам, курсам)				
Число зачетов с разбивкой по семестрам		1/5		1/3
Число экзаменов с разбивкой по семестрам				

Программу составил:
Профессор кафедры ИТСС, д.пол.н. к.т н., доцент Жуковский А.Г.

Рабочая программа дисциплины
«Основы информационной безопасности»

Разработана в соответствии с ФГОС ВО
направления подготовки 11.03.02 ИНФОКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ СВЯЗИ, утвержденным приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 г. N 930.

Составлена на основании учебного плана
направления 11.03.02 Инфокоммуникационные технологии и системы связи _профиля «Защищенные инфокоммуникационные системы», одобренных Учёным советом СКФ МТУСИ, протокол № 8 от 31.03 2026 г., и утвержденных директором СКФ МТУСИ 31.03 2026 г.

Рассмотрена и одобрена на заседании кафедры
«Информационная безопасность»

Протокол от 28.04 2026 г. № 9

И.О. Зав. кафедрой _____ А.Г. Жуковский

1. Цели изучения дисциплины

Целью освоения дисциплины «**Основы информационной безопасности**» является формирование у обучаемых знаний в области основ информационной безопасности и навыков практического обеспечения защиты информации и безопасного использования программных и аппаратных средств в сетях и информационных системах.

2. Планируемые результаты обучения

Изучение дисциплины «**Основы информационной безопасности**» направлено на формирование у обучающегося способности решать следующие профессиональные задачи в соответствии с ***технологическим видом деятельности.***

Результатом освоения дисциплины являются сформированные у обучающегося следующие компетенции:

Компетенции обучающегося, формируемые в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)
ОПК-3: Способен применять методы поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности
Знать:
- понятия информации и информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации; - направления обеспечения информационной безопасности; - классификацию методов криптографического преобразования информации; - структуру и принципы функционирования современных вычислительных систем; - основные способы защиты от потери информации и нарушений работоспособности сетей и систем.
Уметь:
- классифицировать и оценивать угрозы информационной безопасности; - проводить работы по сокрытию информации, проведению резервного копирования, восстановления информации; - использовать механизмы идентификации и аутентификации; - использовать антивирусные средства защиты; - восстанавливать потерянные компьютерные данные; - производить резервное копирование.
Владеть:
- основными понятиями, связанными с обеспечением информационно-психологической безопасности личности, общества и государства; информационного противоборства, информационной войны и формами их проявления в современном мире; - навыками работы по основам защиты информации с использованием программно-аппаратных комплексов.

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):		
1	Б1.О.10	Введение в информационные технологии
2	Б1.О.07	Физика
3	Б1.О.03	Иностранный язык
4	Б1.О.21	Электроника
5	Б1.В.ДВ.01.01	Введение в профессию

Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:		
1	Б1.О.30	Системы искусственного интеллекта
2	Б1.В.06	Инфокоммуникационные системы и сети
3	Б1.В.15	Сетевая безопасность

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 72 часа, 32 часа контактной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компе-тенции	УМИО
1	2	3	4	5	6
Курс 3 , Семестр 5					
Модуль 1. Понятие информационной безопасности. Основные составляющие и направления обеспечения информационной безопасности. (Лек - 8 + ПЗ - 8) = 16 часов контактной работы. 20 часов СР					
1.1	Лекция 1. КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 1. Основные концептуальные положения системы защиты информации 2. Концептуальная модель информационной безопасности 3. Угрозы конфиденциальной информации 4. Действия, приводящие к неправомерному овладении конфиденциальной информацией	Лек	2	ОПК-3	Л1.1 Л1.2 Л1.3
1.2	Лекция 2. НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 1. Правовая защита 2. Организационная защита 3. Инженерно-техническая защита	Лек	2	ОПК-3	Л1.1 Л1.2 Л1.3
1.3	Лекция 3. ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ 1.Общие положения 2.Защита информации от утечки по визуально оптическим каналам 3.Защита информации от утечки по акустическим каналам 4.Защита информации от утечки по электромагнитным каналам 5.Защита информации от утечки по материально - вещественным каналам	Лек	4	ОПК-3	Л1.1 Л1.2 Л1.3
1.4	Практическое занятие 1 Исследование характеристик и возможностей программ по защите и сокрытию файлов, папок	ПЗ	2	ОПК-3	Л3.1

1.5	Практическое занятие 2 Исследование характеристик и возможностей программ по шифрованию, безвозвратному удалению, стеганографии	ПЗ	2	ОПК-3	Л3.1
1.6	Практическое занятие 3 Основные этапы доступа к ресурсам вычислительной системы; использование простого пароля; использование динамически изменяющегося пароля; взаимная проверка подлинности и другие случаи опознания; способы разграничения доступа к компьютерным ресурсам; разграничение доступа по спискам	ПЗ	4	ОПК-3	Л3.1
1.7	Алгоритм симметричной системы шифрования данных – стандарт ГОСТ 28147-89. Алгоритм ассиметричной (двухключевой) системы шифрования данных RSA. Гостехкомиссия России. Руководящий документ Защита от несанкционированного доступа к информации. Термины и Определения. Доктрина информационной безопасности Российской Федерации. Указ президента российской федерации. Об утверждении перечня сведений конфиденциального характера. Положение о лицензировании деятельности по технической защите конфиденциальной информации. Постановление Правительства Российской Федерации от 30 апреля 2002 г. № 290. Инструкция по защите конфиденциальной информации при работе с зарубежными партнерами. Обеспечение сохранения коммерческой тайны предприятия. Каталог обобщенных мероприятий по защите конфиденциальной информации.	СР	20	ОПК-3	Л1.1 Л1.2 Л1.3
Модуль 2 Основы защиты информации в инфокоммуникационных системах и сетях (Лек – 8 + ПЗ – 8) = 16 часов контактной работы 20 часов СР					
2.1	Лекция 4. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ 1. Классификация методов криптографического преобразования информации 2. Шифрование. Основные понятия 3. Методы шифрования с симметричным ключом 4. Системы шифрования с открытым ключом 5. Стандарты шифрования 6. Перспективы использования криптозащиты информации в КС.	Лек	2	ОПК-3	Л1.1 Л1.2 Л1.3
2.2	Лекция 5. СТРУКТУРА И ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ СОВРЕМЕННЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ. Проблемы обеспечения безопасности обработки и	Лек	2	ОПК-3	Л1.1 Л1.2 Л1.3

	хранения информации в вычислительных системах. Базовые этапы построения системы комплексной защиты вычислительных систем. Анализ моделей нарушителя; угрозы информационно-программному обеспечению.				
2.3	Лекция 6. ОСНОВНЫЕ СПОСОБЫ ЗАЩИТЫ ОТ ПОТЕРИ ИНФОРМАЦИИ И НАРУШЕНИЙ РАБОТОСПОСОБНОСТИ СЕТЕЙ И СИСТЕМ 1. Внесение функциональной и информационной избыточности. 2. Способы резервирования информации; правила обновления резервных данных. 3. Методы сжатия информации; архивация файловых данных; резервирование системных данных; подготовка к программной среде.	Лек	4	ОПК-3	Л1.1 Л1.2 Л1.3
2.4	Практическое занятие 4 Исследование характеристик и возможностей антивирусного ПО	ПЗ	2	ОПК-3	Л3.1
2.5	Практическое занятие 5 Исследование характеристик и возможностей программ по восстановлению потерянных данных	ПЗ	2	ОПК-3	Л3.1
2.6	Практическое занятие 6 Исследование характеристик и возможностей программ по организации резервного копирования	ПЗ	4	ОПК-3	Л3.1
2.7	Анализ структуры и принципов функционирования вычислительных сетей с позиции обеспечения информационной безопасности Угрозы информационно-программному обеспечению, характерные только для распределённой вычислительной среды. Классификация компьютерных вирусов Методы и средства борьбы с вирусами Профилактика заражения вирусами компьютерных систем. Порядок действий пользователя при обнаружении заражения ЭВМ вирусами Анализ моделей нарушителя; угрозы информационно-программному обеспечению вычислительных систем и их классификация Основные способы защиты от потери информации и нарушений работоспособности сетей и систем; внесение функциональной и информационной избыточности; способы резервирования информации; правила обновления резервных данных	СРС	20	ОПК-3	Л1.1 Л1.2 Л1.3
3.1	**Зачет**			ОПК-3	Л1.1 Л1.2 Л1.3
Итого – 72 часа					

4.2 Заочная форма обучения, 5 лет (всего 72 часов, 12 часов контактной работы, 60 часов СР

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компе-тенции	УМИО
1	2	3	4	5	6
	Курс 2				
	Модуль 1 – Понятие информационной безопасности. Основные составляющие и направления обеспечения информационной безопасности. – 36 (Лек – 2) = 2 часа контактной работы, 34 часа СР				
1.1	КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 1. Основные концептуальные положения системы защиты информации 2. Концептуальная модель информационной безопасности 3. Угрозы конфиденциальной информации 4. Действия, приводящие к неправомерному овладении конфиденциальной информацией.	Лек.	2	ОПК-3	Л1.1 Л1.2 Л1.3
1.2	НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 1. Правовая защита 2. Организационная защита 3. Инженерно-техническая защита ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ 1.Общие положения 2.Защита информации от утечки по визуально оптическим каналам 3.Защита информации от утечки по акустическим каналам 4.Защита информации от утечки по электромагнитным каналам 5.Защита информации от утечки по материально - вещественным каналам Исследование характеристик и возможностей программ по защите и сокрытию файлов, папок Исследование характеристик и возможностей программ по шифрованию, безвозвратному удалению, стеганографии Основные этапы доступа к ресурсам вычислительной системы; использование простого пароля; использование динамически изменяющегося пароля; взаимная проверка подлинности и другие случаи опознания; способы разграничения доступа к компьютерным ресурсам; разграничение доступа по спискам Алгоритм симметричной системы шифрования данных – стандарт ГОСТ 28147-89. Алгоритм ассиметричной (двухключевой) системы шифрования данных RSA. Гостехкомиссия России. Руководящий документ Защита от несанкционированного доступа к информации. Термины и Определения.	СР	34	ОПК-3	Л1.1 Л1.2 Л1.3

	Доктрина информационной безопасности Российской Федерации. Указ президента российской федерации. Об утверждении перечня сведений конфиденциального характера. Положение о лицензировании деятельности по технической защите конфиденциальной информации. Постановление Правительства Российской Федерации от 30 апреля 2002 г. № 290. Инструкция по защите конфиденциальной информации при работе с зарубежными партнерами. Обеспечение сохранения коммерческой тайны предприятия. Каталог обобщенных мероприятий по защите конфиденциальной информации.				
Модуль 2 Основы защиты информации в инфокоммуникационных системах и сетях – 36 (Лек – 4 + ПЗ - 6) = 10 часов контактной работы, 26 часов СР					
2.1	ОСНОВНЫЕ СПОСОБЫ ЗАЩИТЫ ОТ ПОТЕРИ ИНФОРМАЦИИ И НАРУШЕНИЙ РАБОТОСПОСОБНОСТИ СЕТЕЙ И СИСТЕМ 1. Внесение функциональной и информационной избыточности. 2. Способы резервирования информации; правила обновления резервных данных. 3. Методы сжатия информации; архивация файловых данных; резервирование системных данных; подготовка к программной среде.	Лек.	4	ОПК-3	Л3-1
2.2	Основные этапы доступа к ресурсам вычислительной системы; использование простого пароля; использование динамически изменяющегося пароля; взаимная проверка подлинности и другие случаи опознания; способы разграничения доступа к компьютерным ресурсам.	ПЗ	2	ОПК-3	Л3-1
2.3	Исследование характеристик и возможностей программ по восстановлению потерянных данных	ПЗ	2	ОПК-3	Л3-1
2.4	Исследование характеристик и возможностей программ по организации резервного копирования	ПЗ	2	ОПК-3	Л3-1
2.5	КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ 1. Классификация методов криптографического преобразования информации 2. Шифрование. Основные понятия 3. Методы шифрования с симметричным ключом 4. Системы шифрования с открытым ключом 5. Стандарты шифрования 6. Перспективы использования криптозащиты информации в КС. СТРУКТУРА И ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ СОВРЕМЕННЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ. Проблемы обеспечения безопасности обработки и хранения информации в вычислительных системах.	СР	26	ОПК-3	Л1.1 Л1.2 Л1.3

	Базовые этапы построения системы комплексной защиты вычислительных систем. Анализ моделей нарушителя; угрозы информационно-программному обеспечению. Исследование характеристик и возможностей антивирусного ПО Анализ структуры и принципов функционирования вычислительных сетей с позиции обеспечения информационной безопасности Угрозы информационно-программному обеспечению, характерные только для распределённой вычислительной среды. Классификация компьютерных вирусов Методы и средства борьбы с вирусами Профилактика заражения вирусами компьютерных систем. Порядок действий пользователя при обнаружении заражения ЭВМ вирусами Анализ моделей нарушителя; угрозы информационно-программному обеспечению вычислительных систем и их классификация Основные способы защиты от потери информации и нарушений работоспособности сетей и систем; внесение функциональной и информационной избыточности; способы резервирования информации; правила обновления резервных данных				
3.1	**Зачет**			ОПК-3	Л1.1 Л1.2 Л1.3
Итого – 72 часа					

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Рекомендуемая литература				
5.1.1. Основная литература				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л1.1	Галатенко, В. А.	Основы информационной безопасности : учебное пособие	Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024.	Э1
Л1.2	Гультяева, Т. А.	Основы информационной безопасности : учебное пособие	Новосибирск : Новосибирский государственный технический университет, 2018	Э2
Л1.3	Суворова, Г. М.	Информационная безопасность : учебное пособие	Саратов : Вузовское образование, 2024.	Э3
5.1.2. Дополнительная литература				

Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л2.1	Фаронов, А. Е.	Основы информационной безопасности при работе на компьютере : учебное пособие	Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024.	Э4

5.1.3. Учебно-методическое обеспечение для самостоятельной работы обучающихся

Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л3.1	Жуковский А.Г., Жуковский Д.А., Швидченко С.А.	ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕЙ И СИСТЕМ. Учебное пособие. – Ростов-на-Дону: СКФ МТУСИ, 2020. – 52 с.	РнД: СКФ МТУСИ, 2020	Э5
Л3.2	Компания «Перспективный мониторинг»	Руководства руководителя, группы мониторинга, группы реагирования	Компания «Перспективный мониторинг»	Э6

5.2. Электронные образовательные ресурсы

Э1	https://www.iprbookshop.ru/142285.html
Э2	https://www.iprbookshop.ru/91640.html
Э3	https://www.iprbookshop.ru/142805.html
Э4	https://www.iprbookshop.ru/133957.html
Э5	https://elib.mtuci.ru/view.php?book_id=170004
Э6	https://amonitoring.ru/article/

5.3. Программное обеспечение

П.1	1. AVAST Free Antivirus 2. AVG AntiVirus Free 3. Dr.Web Antivirus 4. Антивирус Касперского 5. ESET NOD32 Антивирус 6. AVZ Antivirus 7. Avira Free Antivirus 8. Norton AntiVirus 9. McAfee Antivirus 10. Emsisoft Anti-Malware 11. BullGuard Antivirus 12. Protector Plus Antivirus 13. Panda Antivirus 14. Ashampoo Anti-Virus 14. G Data AntiVirus 16. K7 AntiVirus 17. VIRUSfighter 18. Twister Antivirus	Антивирусное ПО. Свободное, условно свободное или триал-версии.
П.2	1. Wise Folder Hider 2. Secure Folders 3. Anvide Lock Folder 4. Folder Lock 5. Easy File Locker	Программное обеспечение по защите и сокрытию файлов и папок. Свободное, условно свободное или триал-версии.

	6. Folder Guard	
	7. DEKSI USB Security	
	8. Locker (защита папок и дисков)	
	9. Advanced Hider	
	10. Hide Folders XP	
	11. Hide Files	
П.3	1. TrustPort Tools	Программное обеспечение по шифрованию, безвозвратному удалению, стеганографии. Свободное, условно свободное или триал-версии.
	2. Cryptic Disk	
	3. Locker (скрытие файлов)	
	4. Max File Encryption	
	5. Secure Disk	
	6. Masker 7.1	
	7. Fox Secret	
	8. HideInPicture 1.0	
	9. Шифровальщик	
	10. Advanced Encryption Package	
	11. Gpg4win	
	12. Cryptic Disk Professional	
	13. CyberSafe Files Encryption	
	14. Steganos Privacy Suite	
	15. Lavasoft Privacy Toolbox	
	16. pkiImage Free Edition	
П.4	1. Hetman Partition Recovery	Программное обеспечение по восстановлению данных. Свободное, условно свободное или триал-версии.
	2. Active File Recovery	
	3. R-Studio 7.6	
	4. Auslogics File Recovery	
	5. Active UNDELETE	
	6. Paragon Rescue Kit	
	7. Wise Data Recovery	
	8. Puran File Recovery	
	9. O&O DiskRecovery	
	10. Tenorshare Any Data Recovery	
	11. Power Data Recovery	
	12. GetDataBack	
	13. Recover My Files	
	14. R-Undelete	
	15. Handy Recovery	
	16. Ashampoo Undeleter	
П.5	1. Iperius Backup	Программное обеспечение по резервному копированию данных. Свободное, условно свободное или триал-версии.
	2. FBackup	
	3. Backup4all	
	4. Uranium Backup Free	
	5. Simple Data Backup	
	6. Personal Backup	
	7. Back4Sure	
	8. SyncBackFree	
	9. Handy Backup	

	10. EASEUS Todo Backup 8.0 Free Edition	
	11. Exiland Backup Free 4.0	
	12. Nero BackItUp	
	13. Paragon Rescue Kit 14.0 Free	
	14. Action Backup	
	15. LimBackup	
	16. AVSbackup	
	17. ExtraBackup	
	18. Cobian Backup	
	19. Backup & Recovery 10 Build 9169 Free Edition	
	20. Information Backup System	
П.6	MS Office – с лицензией	

6. Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий	
1	Лекционная аудитория, оснащенная интерактивной доской, проектором, ПК (ноутбуком), экраном.
6.2 МТО лабораторных работ и практических занятий	
1	Лаборатория «Программно-аппаратные средства защиты информации», укомплектованная специализированной мебелью, оснащенную программно-аппаратными комплексами защиты информации, включающими в том числе средства криптографической защиты информации,
2	Лаборатория «Технической защиты информации», укомплектованная специализированной мебелью, оснащенная техническими средствами защиты информации
3	Учебные аудитории, оборудованные компьютерной техникой, с возможностью подключения к сети «Интернет», и обеспечением доступа в электронную информационно-образовательную среду СКФ МТУСИ
6.3 МТО рубежных контролей, экзамена	
1	Учебные аудитории, оборудованные компьютерной техникой, с возможностью подключения к сети «Интернет», и обеспечением доступа в электронную информационно-образовательную среду СКФ МТУСИ
6.4 МТО самостоятельной работы обучающихся	
1	Помещение для самостоятельной работы обучающихся оснащено компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду СКФ МТУСИ

7. Оценочные материалы
Оценочные материалы и перечень видов оценочных средств текущего контроля и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

8. Методические рекомендации для обучающихся по освоению дисциплины
Методические рекомендации по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.

9. Особенности реализации дисциплины (модуля) при обучении инвалидов и лиц с ограниченными возможностями здоровья

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков.

Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания.

Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.).

Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь.

Текущий контроль успеваемости осуществляется в устной форме.

При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).

10. Дополнения и изменения в Рабочей программе

Лист актуализации рабочей программы дисциплины
«Основы информационной безопасности Б1.О.24»
для использования в 20___/20____ учебном году

Утверждаю
Зам. директора по УР _____ Н.А. Андреева

_____ 20_____ г.

Направление: 11.03.02 Инфокоммуникационные технологии и системы связи
Профиль: «Защищенные инфокоммуникационные системы»
Форма обучения: очно-заочная

(Возможны следующие варианты):
а) Рабочая программа действует без изменений.
б) В рабочую программу вносятся следующие изменения:
1) ……..;
2) ……..;
3) ……

Разработчик (и): _____
(ФИО, ученая степень, ученое звание)
«__» _____20___г.

Рабочая программа пересмотрена и одобрена на заседании кафедры _____

Протокол № _____ от «__» _____20____г.

Заведующий кафедрой _____

Приложение 1

Оценочные материалы для проведения текущего контроля и промежуточной аттестации по дисциплине

1. Оценочные материалы для проведения промежуточной аттестации по дисциплине

1.1 Шкала оценивания компетенций

Шкала оценивания компетенций		
Оценка	**Уровень освоения компетенции**	**Критерии оценивания**
«Отлично»	Высокий уровень	Обучающийся показывает всестороннее, систематическое и глубокое знание основного и дополнительного учебного материала, умеет свободно выполнять задания, предусмотренные программой; усвоил основную и знаком с дополнительной рекомендованной литературой; может объяснить взаимосвязь основных понятий дисциплины в их значении для последующей профессиональной деятельности; проявляет творческие способности в понимании, изложении и использовании учебного материала.
«Хорошо»	Повышенный уровень	Обучающийся показывает достаточный уровень знаний в пределах основного учебного материала, без существенных ошибок выполняет предусмотренные в программе задания; усвоил основную литературу, рекомендованную в программе; способен объяснить взаимосвязь основных понятий дисциплины при дополнительных вопросах преподавателя. Допускает не существенные погрешности в ответах, устраняет их без помощи преподавателя.
«Удовлетворительно»	Пороговый уровень	Обучающийся показывает знания основного учебного материала в минимальном объеме, необходимом для дальнейшей учебы; справляется с выполнением заданий, предусмотренных программой, допуская при этом большое количество не принципиальных ошибок; знаком с основной литературой, рекомендованной программой. Допускает существенные погрешности в ответах, но обладает необходимыми знаниями для их устранения под руководством преподавателя.
«Неудовлетворительно»	Минимальный уровень не достигнут	Обучающийся обнаруживает пробелы в знаниях основного учебного материала, допускает принципиальные ошибки в

		выполнении предусмотренных программой заданий, не знаком с рекомендованной литературой, не может исправить допущенные ошибки. Как правило, оценка «неудовлетворительно» ставится обучающимся, которые не могут продолжить обучение или приступить к профессиональной деятельности по окончании вуза без дополнительных занятий по соответствующей дисциплине.

1.2 Показатели, критерии и шкалы оценивания компетенций

Показатели компетенции	Критерии оценивания	Шкала оценивания
ОПК-3		
Знать:		
- понятия информации и информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации; - направления обеспечения информационной безопасности;	Контрольная работа	Модуль 1 0÷10 «Неудовлетворительно» -0-3 «Удовлетворительно» - 4-6 «Хорошо» - 7-8- «Отлично» - 9-10
- классификацию методов криптографического преобразования информации; - структуру и принципы функционирования современных вычислительных систем; - основные способы защиты от потери информации и нарушений работоспособности сетей и систем	Контрольная работа	Модуль 2 0÷10 «Неудовлетворительно» -0-4 «Удовлетворительно» - 5-6 «Хорошо» - 7-8 «Отлично» - 9-10
Уметь		
- классифицировать и оценивать угрозы информационной безопасности; - проводить работы по сокрытию информации, проведению резервного копирования, восстановления информации; - использовать механизмы идентификации и аутентификации;	Практическое занятие 1-3	Модуль 1 0÷20 «Неудовлетворительно» -0-7 «Удовлетворительно» - 8-12 «Хорошо» - 13-16 «Отлично» - 17-20
- использовать антивирусные средства защиты; - восстанавливать потерянные компьютерные данные; - производить резервное копирование.	Практическое занятие 4-6	Модуль 2 0÷20 «Неудовлетворительно» -0-7 «Удовлетворительно» - 8-12 «Хорошо» - 13-16 «Отлично» - 17-20
Владеть		

- основными понятиями, связанными с обеспечением информационно-психологической безопасности личности, общества и государства; информационного противоборства, информационной войны и формами их проявления в современном мире;	Практическое занятие 1-3	Модуль 1 0÷20 «Неудовлетворительно» -0-7 «Удовлетворительно» - 8-12 «Хорошо» - 13-16 «Отлично» - 17-20
- навыками работы по основам защиты информации с использованием программно-аппаратных комплексов	Практическое занятие 4-6	Модуль 2 0÷20 «Неудовлетворительно» -0-7 «Удовлетворительно» - 8-12 «Хорошо» - 13-16 «Отлично» - 17-20
Зачет		41-100 баллов – зачет менее 41 балла - незачет

1.3 Оценочные материалы: типовые контрольные задания, иные материалы

1.3.1 Оценочные средства для очной формы обучения

Модуль 1 (50 баллов):

Модуль содержит 3 лекционных занятия и 3 практических занятия. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 10. За выполненные практические работы студент получает максимум 40 баллов. Общее максимальное количество баллов за модуль 1 составляет 50.

Вопросы для контрольной работы (ОПК-3):

1. Основные концептуальные положения системы защиты информации
2. Концептуальная модель информационной безопасности
3. Угрозы конфиденциальной информации
4. Действия, приводящие к неправомерному овладении конфиденциальной информацией
5. Правовая защита
6. Организационная защита
7. Инженерно-техническая защита
8.Общие положения
9.Защита информации от утечки по визуально оптическим каналам
10.Защита информации от утечки по акустическим каналам
11.Защита информации от утечки по электромагнитным каналам
12.Защита информации от утечки по материально - вещественным каналам
13. Классификация методов криптографического преобразования информации
14. Шифрование. Основные понятия

15. Методы шифрования с симметричным ключом

16. Системы шифрования с открытым ключом

17. Стандарты шифрования

18. Перспективы использования криптозащиты информации в КС.

Практическое занятие 1. Исследование характеристик и возможностей программ по защите и сокрытию файлов, папок

Контрольные вопросы ПЗ№1 (ОПК-3):

1. Укажите назначение, достоинства и недостатки программы Wise Folder Hider.

2. Укажите назначение, достоинства и недостатки программы Secure Folders

3. Укажите назначение, достоинства и недостатки программы Anvide Lock Folder

4. Укажите назначение, достоинства и недостатки программы Folder Lock

5. Укажите назначение, достоинства и недостатки программы Easy File Locker

6. Укажите назначение, достоинства и недостатки программы Folder Guard

7. Укажите назначение, достоинства и недостатки программы DEKSI USB Security

8. Укажите назначение, достоинства и недостатки программы Locker

9. Укажите назначение, достоинства и недостатки программы Advanced Hider

10. Укажите назначение, достоинства и недостатки программы Hide Folders XP

11. Укажите назначение, достоинства и недостатки программы Hide Files

Практическое занятие 2. Исследование характеристик и возможностей программ по шифрованию, безвозвратному удалению, стеганографии

Контрольные вопросы ПЗ№2 (ОПК-3):

1. Укажите назначение, достоинства и недостатки программы TrustPort Tools

2. Укажите назначение, достоинства и недостатки программы Cryptic Disk

3. Укажите назначение, достоинства и недостатки программы Locker (скрытие файлов)

4. Укажите назначение, достоинства и недостатки программы Max File Encryption

5. Укажите назначение, достоинства и недостатки программы Secure Disk

6. Укажите назначение, достоинства и недостатки программы Masker 7.1

7. Укажите назначение, достоинства и недостатки программы Fox Secret

8. Укажите назначение, достоинства и недостатки программы HideInPicture 1.0

9. Укажите назначение, достоинства и недостатки программы Шифровальщик

10. Укажите назначение, достоинства и недостатки программы Advanced Encryption Package

11. Укажите назначение, достоинства и недостатки программы Gpg4win

12. Укажите назначение, достоинства и недостатки программы Cryptic Disk Professional

13. Укажите назначение, достоинства и недостатки программы CyberSafe Files Encryption

14. Укажите назначение, достоинства и недостатки программы Steganos Privacy Suite

15. Укажите назначение, достоинства и недостатки программы Lavasoft Privacy Toolbox

16. Укажите назначение, достоинства и недостатки программы pkiImage Free Edition

Практическое занятие 3. Основные этапы доступа к ресурсам вычислительной системы; использование простого пароля; использование динамически изменяющегося пароля; взаимная проверка подлинности и другие случаи опознания; способы разграничения доступа к компьютерным ресурсам; разграничение доступа по спискам

Контрольные вопросы ПЗ№3 (ОПК-3):

1. Политика информационной безопасности предприятия и организации.

2. Правовые (организационно-технические, экономические) методы обеспечения информационной безопасности.

3. Обеспечение информационной безопасности компьютерных систем.

4. Анализ современных подходов к построению систем защиты информации.

5. Критерии оценки защищенности компьютерных систем, методы и средства обеспечения их информационной безопасности.

6. Особенности обеспечения информационной безопасности компьютерных систем при обработке информации, составляющей государственную тайну.

7. Обеспечение безопасности технических систем и человека в условиях использования информационного оружия.

8. Анализ факторов, определяющих безопасность технических систем.

9. Классификация и возможности технических разведок.

10. Показатели защищенности средств вычислительной техники от НСД к информации.

11. Пароль как средство защиты от НСД.

12. Требования по защите информации в автоматизированных системах от НСД.

13. Оценка безопасности информационных технологий по Общим критериям.

Модуль 2: (50 баллов):

Модуль содержит 3 лекционных занятия и 3 практических занятия. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 10. За выполненные и защищенные практические работы студент получает максимум 40 баллов. Общее максимальное количество баллов за модуль 1 составляет 50.

Вопросы для контрольной работы (ОПК-3):

1. Проблемы обеспечения безопасности обработки информации.

2. Проблемы обеспечения безопасности хранения информации в вычислительных системах.

3. Базовые этапы построения системы комплексной защиты вычислительных систем.

4. Анализ моделей нарушителя

5. Угрозы информационно-программному обеспечению

6. Классификация компьютерных вирусов

7. Файловые вирусы

8. Загрузочные вирусы

9. Вирусы и операционные системы

10. Методы и средства борьбы с вирусами

11. Профилактика заражения вирусами компьютерных

12. Порядок действий пользователя при обнаружении заражения ЭВМ вирусами

13. Внесение функциональной и информационной избыточности.

14. Понятие надежности

15. Способы резервирования информации

16. Правила обновления резервных данных

17. Методы сжатия информации

18. Архивация файловых данных

19. Резервирование системных данных

ПЗ №4. Исследование характеристик и возможностей антивирусного ПО

Контрольные вопросы ПЗ№4 (ОПК-3):

1. Укажите назначение, достоинства и недостатки программы AVAST Free Antivirus

2. Укажите назначение, достоинства и недостатки программы AVG AntiVirus Free

3. Укажите назначение, достоинства и недостатки программы Dr.Web Antivirus

4. Укажите назначение, достоинства и недостатки программы Антивирус Касперского

5. Укажите назначение, достоинства и недостатки программы ESET NOD32 Антивирус

6. Укажите назначение, достоинства и недостатки программы AVZ Antivirus

7. Укажите назначение, достоинства и недостатки программы Avira Free Antivirus

8. Укажите назначение, достоинства и недостатки программы Norton AntiVirus

9. Укажите назначение, достоинства и недостатки программы McAfee Antivirus

10. Укажите назначение, достоинства и недостатки программы Emsisoft Anti-Malware

11. Укажите назначение, достоинства и недостатки программы BullGuard Antivirus

12. Укажите назначение, достоинства и недостатки программы Protector Plus Antivirus

13. Укажите назначение, достоинства и недостатки программы Panda Antivirus

14. Укажите назначение, достоинства и недостатки программы Ashampoo Anti-Virus

14. Укажите назначение, достоинства и недостатки программы G Data AntiVirus

16. Укажите назначение, достоинства и недостатки программы K7 AntiVirus

17. Укажите назначение, достоинства и недостатки программы VIRUSfighter

18. Укажите назначение, достоинства и недостатки программы Twister Antivirus

ПЗ №5. Исследование характеристик и возможностей программ по восстановлению потерянных данных

Контрольные вопросы ПЗ№5 (ОПК-3):

1. Укажите назначение, достоинства и недостатки программы Hetman Partition Recovery

2. Укажите назначение, достоинства и недостатки программы Active File Recovery

3. Укажите назначение, достоинства и недостатки программы R-Studio 7.6

4. Укажите назначение, достоинства и недостатки программы Auslogics File Recovery

5. Укажите назначение, достоинства и недостатки программы Active UNDELETE

6. Укажите назначение, достоинства и недостатки программы Paragon Rescue Kit

7. Укажите назначение, достоинства и недостатки программы Wise Data Recovery

8. Укажите назначение, достоинства и недостатки программы Puran File Recovery

9. Укажите назначение, достоинства и недостатки программы O&O DiskRecovery

10. Укажите назначение, достоинства и недостатки программы Tenorshare Any Data Recovery

11. Укажите назначение, достоинства и недостатки программы Power Data Recovery

12. Укажите назначение, достоинства и недостатки программы GetDataBack

13. Укажите назначение, достоинства и недостатки программы Recover My Files

14. Укажите назначение, достоинства и недостатки программы R-Undelete

15. Укажите назначение, достоинства и недостатки программы Handy Recovery

16. Укажите назначение, достоинства и недостатки программы Ashampoo Undeleter

ПЗ №6. Исследование характеристик и возможностей программ по организации резервного копирования

Контрольные вопросы ПЗ№6 (ОПК-3):

1. Укажите назначение, достоинства и недостатки программы Iperius Backup

2. Укажите назначение, достоинства и недостатки программы FBackup

3. Укажите назначение, достоинства и недостатки программы Backup4all

4. Укажите назначение, достоинства и недостатки программы Uranium Backup Free

5. Укажите назначение, достоинства и недостатки программы Simple Data Backup

6. Укажите назначение, достоинства и недостатки программы Personal Backup

7. Укажите назначение, достоинства и недостатки программы Back4Sure

8. Укажите назначение, достоинства и недостатки программы SyncBackFree

9. Укажите назначение, достоинства и недостатки программы Handy Backup

10. Укажите назначение, достоинства и недостатки программы EASEUS Todo Backup 8.0 Free Edition

11. Укажите назначение, достоинства и недостатки программы Exiland Backup Free 4.0

12. Укажите назначение, достоинства и недостатки программы Nero BackItUp

13. Укажите назначение, достоинства и недостатки программы Paragon Rescue Kit 14.0 Free

14. Укажите назначение, достоинства и недостатки программы Action Backup

15. Укажите назначение, достоинства и недостатки программы LimBackup

16. Укажите назначение, достоинства и недостатки программы AVSbackup

17. Укажите назначение, достоинства и недостатки программы ExtraBackup

18. Укажите назначение, достоинства и недостатки программы Cobian Backup

19. Укажите назначение, достоинства и недостатки программы Backup & Recovery 10 Build 9169 Free Edition

20. Укажите назначение, достоинства и недостатки программы Information Backup System

1.3.2.Вопросы, выносимые на зачет по дисциплине «Основы информационной безопасности» (ОПК-3)

1. Понятие и сущность ЗИ. Назначение ЗИ. Задачи ЗИ.
2. Методологические основы организации ЗИ.
3. Принципы организации ЗИ. Основные требования, предъявляемые к ЗИ.
4. Правовое регулирование в области безопасности информации.
5. Общая характеристика организационных методов защиты информации.
6. Основные факторы, влияющие на организацию ЗИ.
7. Функции руководства предприятия и подразделений предприятия, экспертной комиссии, службы защиты информации.
8. Классификация информации по видам тайны и степеням конфиденциальности. Нормативное закрепление состава защищаемой информации; структура перечней сведений, относимых к различным видам тайны.
9. Значение носителей защищаемой информации как объектов защиты. Факторы, определяющие состав носителей информации.
10. Методика выявления состава носителей защищаемой информации. Хранилища носителей информации как объект защиты.
11. Особенности помещений для работы с защищаемой информацией как объектов защиты.
12. Состав технических средств обработки, передачи, транспортировки и защиты информации, являющихся объектами защиты.
13. Определение возможных методов несанкционированного доступа к защищаемой информации.
14. Методика выявления нарушителей (незаконных пользователей) и состава интересующей их информации.
15. Факторы, влияющие на выбор компонентов ЗИ. Объекты защиты как основной фактор,

определяющий состав компонентов ЗИ.

16. Обеспечение полноты составляющих защиты. Учет всех факторов и обстоятельств, оказывающих влияние на качество защиты.
17. Обеспечение безопасности всей совокупности подлежащей защите информации во всех компонентах ее сбора, хранения, передачи и использования, а также во все время и при всех режимах функционирования систем обработки информации.
18. Понятие модели объекта, основные виды моделей и их характеристика.
19. Распределение функций по защите информации между руководством предприятия, службой защиты информации, обеспечение взаимодействия между ними.
20. Разработка нормативных документов, регламентирующих деятельность персонала по защите информации. Подбор и обучение персонала.
21. Состав нормативно-методических документов по обеспечению функционирования системы ЗИ.
22. Содержание и особенности экспертной оценки эффективности защиты.
23. Сведения, составляющие коммерческую тайну предприятия
24. Угрозы безопасности информации в компьютерных системах.
25. Угрозы для протоколов и служб Internet
26. Виртуальные частные сети и их информационная защита
27. Методы идентификации и аутентификации пользователей
28. Межсетевые экраны
29. Оценка защищенности информации от утечки по каналам ПЭМИН
30. Основные концептуальные положения системы защиты информации
31. Действия, приводящие к неправомерному овладению конфиденциальной информацией
32. Направления обеспечения безопасности
33. Правовые документы по защите информации и их характеристика
34. Задачи по обеспечению организационных мероприятий по защите информации.
35. Классификация мер инженерно-технической защиты информации.
36. Классификация инженерно-технической защиты информации по техническим средствам.
37. Классификация программных средств защиты информации
38. Каналы разглашения конфиденциальной информации.
39. Способы пресечения разглашения информации.
40. Каналы утечки конфиденциальной информации. Их классификация.
41. Защита информации от утечки по визуально-оптическим каналам
42. Защита информации от утечки но акустическим каналам
43. Защита информации от утечки по электромагнитным каналам
44. Способы несанкционированного доступа
45. Защита от наблюдения и фотографирования

46. Способы прослушивания посредством радиозакладок.
47. Обеспечение безопасности телефонных переговоров
48. Назначение и характеристики нелинейных локаторов
49. Назначение и характеристики средств постановки активных помех
50. Назначение и принцип работы скремблеров (дескремблеров)
51. Противодействие незаконному подключению к линиям связи
52. Меры защиты от радиоперехвата
53. Основные встроенные механизмы защиты ОС и их недостатки
54. Анализ существующих угроз для современных универсальных ОС
55. Задачи и методы резервирования.
56. Криптографические методы защиты информации.
57. Компьютерные вирусы и механизмы борьбы с ними.
58. Профилактика заражения вирусами компьютерных систем.

1.4. Оценочные материалы для заочной формы обучения

Вопросы для контрольной работы 1. (ОПК-3):

1. Основные концептуальные положения системы защиты информации
2. Концептуальная модель информационной безопасности
3. Угрозы конфиденциальной информации
4. Действия, приводящие к неправомерному овладении конфиденциальной информацией
5. Правовая защита
6. Организационная защита
7. Инженерно-техническая защита
8. Общие положения
9. Защита информации от утечки по визуально оптическим каналам
10. Защита информации от утечки по акустическим каналам
11. Защита информации от утечки по электромагнитным каналам
12. Защита информации от утечки по материально - вещественным каналам
13. Классификация методов криптографического преобразования информации
14. Шифрование. Основные понятия
15. Методы шифрования с симметричным ключом
16. Системы шифрования с открытым ключом
17. Стандарты шифрования
18. Перспективы использования криптозащиты информации в КС.

Практическое занятие 3. Основные этапы доступа к ресурсам вычислительной системы; использование простого пароля; использование динамически изменяющегося пароля; взаимная проверка подлинности и другие случаи опознания; способы разграничения доступа к компьютерным ресурсам; разграничение доступа по спискам

Контрольные вопросы ПЗ№3 (ОПК-3):

1. Политика информационной безопасности предприятия и организации.

2. Правовые (организационно-технические, экономические) методы обеспечения информационной безопасности.

3. Обеспечение информационной безопасности компьютерных систем.

4. Анализ современных подходов к построению систем защиты информации.

5. Критерии оценки защищенности компьютерных систем, методы и средства обеспечения их информационной безопасности.

6. Особенности обеспечения информационной безопасности компьютерных систем при обработке информации, составляющей государственную тайну.

7. Обеспечение безопасности технических систем и человека в условиях использования информационного оружия.

8. Анализ факторов, определяющих безопасность технических систем.

9. Классификация и возможности технических разведок.

10. Показатели защищенности средств вычислительной техники от НСД к информации.

11. Пароль как средство защиты от НСД.

12. Требования по защите информации в автоматизированных системах от НСД.

13. Оценка безопасности информационных технологий по Общим критериям.

Вопросы для контрольной работы 2 (ОПК-3):

1. Проблемы обеспечения безопасности обработки информации.

2. Проблемы обеспечения безопасности хранения информации в вычислительных системах.

3. Базовые этапы построения системы комплексной защиты вычислительных систем.

4. Анализ моделей нарушителя

5. Угрозы информационно-программному обеспечению

6. Классификация компьютерных вирусов

7. Файловые вирусы

8. Загрузочные вирусы

9. Вирусы и операционные системы

10. Методы и средства борьбы с вирусами

11. Профилактика заражения вирусами компьютерных

12. Порядок действий пользователя при обнаружении заражения ЭВМ вирусами

13. Внесение функциональной и информационной избыточности.

14. Понятие надежности

15. Способы резервирования информации

16. Правила обновления резервных данных

17. Методы сжатия информации

18. Архивация файловых данных

19. Резервирование системных данных

ПЗ №5. Исследование характеристик и возможностей программ по восстановлению потерянных данных

Контрольные вопросы ПЗ№5 (ОПК-3):

1. Укажите назначение, достоинства и недостатки программы Hetman Partition Recovery

2. Укажите назначение, достоинства и недостатки программы Active File Recovery

3. Укажите назначение, достоинства и недостатки программы R-Studio 7.6

4. Укажите назначение, достоинства и недостатки программы Auslogics File Recovery

5. Укажите назначение, достоинства и недостатки программы Active UNDELETE

6. Укажите назначение, достоинства и недостатки программы Paragon Rescue Kit

7. Укажите назначение, достоинства и недостатки программы Wise Data Recovery

8. Укажите назначение, достоинства и недостатки программы Puran File Recovery

9. Укажите назначение, достоинства и недостатки программы O&O DiskRecovery

10. Укажите назначение, достоинства и недостатки программы Tenorshare Any Data Recovery

11. Укажите назначение, достоинства и недостатки программы Power Data Recovery

12. Укажите назначение, достоинства и недостатки программы GetDataBack

13. Укажите назначение, достоинства и недостатки программы Recover My Files

14. Укажите назначение, достоинства и недостатки программы R-Undelete

15. Укажите назначение, достоинства и недостатки программы Handy Recovery

16. Укажите назначение, достоинства и недостатки программы Ashampoo Undeleter

ПЗ №6. Исследование характеристик и возможностей программ по организации резервного копирования

Контрольные вопросы ПЗ№6 (ОПК-3):

1. Укажите назначение, достоинства и недостатки программы Iperius Backup

2. Укажите назначение, достоинства и недостатки программы FBackup

3. Укажите назначение, достоинства и недостатки программы Backup4all

4. Укажите назначение, достоинства и недостатки программы Uranium Backup Free

5. Укажите назначение, достоинства и недостатки программы Simple Data Backup

6. Укажите назначение, достоинства и недостатки программы Personal Backup

7. Укажите назначение, достоинства и недостатки программы Back4Sure

8. Укажите назначение, достоинства и недостатки программы SyncBackFree

9. Укажите назначение, достоинства и недостатки программы Handy Backup

10. Укажите назначение, достоинства и недостатки программы EASEUS Todo Backup 8.0 Free Edition

11. Укажите назначение, достоинства и недостатки программы Exiland Backup Free 4.0

12. Укажите назначение, достоинства и недостатки программы Nero BackItUp

13. Укажите назначение, достоинства и недостатки программы Paragon Rescue Kit 14.0 Free

14. Укажите назначение, достоинства и недостатки программы Action Backup

15. Укажите назначение, достоинства и недостатки программы LimBackup

16. Укажите назначение, достоинства и недостатки программы AVSbackup

17. Укажите назначение, достоинства и недостатки программы ExtraBackup

18. Укажите назначение, достоинства и недостатки программы Cobian Backup

19. Укажите назначение, достоинства и недостатки программы Backup & Recovery 10 Build 9169 Free Edition

20. Укажите назначение, достоинства и недостатки программы Information Backup System

Вопросы, выносимые на зачет по дисциплине «Основы информационной безопасности» (ОПК-3)

1. Понятие и сущность ЗИ. Назначение ЗИ. Задачи ЗИ.
2. Методологические основы организации ЗИ.
3. Принципы организации ЗИ. Основные требования, предъявляемые к ЗИ.
4. Правовое регулирование в области безопасности информации.
5. Общая характеристика организационных методов защиты информации.
6. Основные факторы, влияющие на организацию ЗИ.
7. Функции руководства предприятия и подразделений предприятия, экспертной комиссии, службы защиты информации.
8. Классификация информации по видам тайны и степеням конфиденциальности. Нормативное закрепление состава защищаемой информации; структура перечней сведений, относимых к различным видам тайны.
9. Значение носителей защищаемой информации как объектов защиты. Факторы, определяющие состав носителей информации.
10. Методика выявления состава носителей защищаемой информации. Хранилища носителей информации как объект защиты.
11. Особенности помещений для работы с защищаемой информацией как объектов

защиты.

12. Состав технических средств обработки, передачи, транспортировки и защиты информации, являющихся объектами защиты.

13. Определение возможных методов несанкционированного доступа к защищаемой информации.

14. Методика выявления нарушителей (незаконных пользователей) и состава интересующей их информации.

15. Факторы, влияющие на выбор компонентов ЗИ. Объекты защиты как основной фактор, определяющий состав компонентов ЗИ.

16. Обеспечение полноты составляющих защиты. Учет всех факторов и обстоятельств, оказывающих влияние на качество защиты.

17. Обеспечение безопасности всей совокупности подлежащей защите информации во всех компонентах ее сбора, хранения, передачи и использования, а также во все время и при всех режимах функционирования систем обработки информации.

18. Понятие модели объекта, основные виды моделей и их характеристика.

19. Распределение функций по защите информации между руководством предприятия, службой защиты информации, обеспечение взаимодействия между ними.

20. Разработка нормативных документов, регламентирующих деятельность персонала по защите информации. Подбор и обучение персонала.

21. Состав нормативно-методических документов по обеспечению функционирования системы ЗИ.

22. Содержание и особенности экспертной оценки эффективности защиты.

23. Сведения, составляющие коммерческую тайну предприятия

24. Угрозы безопасности информации в компьютерных системах.

25. Угрозы для протоколов и служб Internet

26. Виртуальные частные сети и их информационная защита

27. Методы идентификации и аутентификации пользователей

28. Межсетевые экраны

29. Оценка защищенности информации от утечки по каналам ПЭМИН

30. Основные концептуальные положения системы защиты информации

31. Действия, приводящие к неправомерному овладению конфиденциальной информацией

32. Направления обеспечения безопасности

33. Правовые документы по защите информации и их характеристика

34. Задачи по обеспечению организационных мероприятий по защите информации.

35. Классификация мер инженерно-технической защиты информации.

36. Классификация инженерно-технической защиты информации по техническим средствам.

37. Классификация программных средств защиты информации

38. Каналы разглашения конфиденциальной информации.
39. Способы пресечения разглашения информации.
40. Каналы утечки конфиденциальной информации. Их классификация.
41. Защита информации от утечки по визуально-оптическим каналам
42. Защита информации от утечки но акустическим каналам
43. Защита информации от утечки по электромагнитным каналам
44. Способы несанкционированного доступа
45. Защита от наблюдения и фотографирования
46. Способы прослушивания посредством радиозакладок.
47. Обеспечение безопасности телефонных переговоров
48. Назначение и характеристики нелинейных локаторов
49. Назначение и характеристики средств постановки активных помех
50. Назначение и принцип работы скремблеров (дескремблеров)
51. Противодействие незаконному подключению к линиям связи
52. Меры защиты от радиоперехвата
53. Основные встроенные механизмы защиты ОС и их недостатки
54. Анализ существующих угроз для современных универсальных ОС
55. Задачи и методы резервирования.
56. Криптографические методы защиты информации.
57. Компьютерные вирусы и механизмы борьбы с ними.
58. Профилактика заражения вирусами компьютерных систем.

2 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

2.1.Порядок и методика проведения текущего контроля и промежуточной аттестации

Предусмотрены следующие виды контроля:

- текущий контроль по каждому модулю – в форме написания контрольной работы для оценки теоретических знаний;

- текущий контроль по каждому модулю – в форме отчетов по лабораторным работам и практическим занятиям для оценки практических навыков;

- промежуточная аттестация - контроль усвоенных по дисциплине компетенций за период ее изучения - в форме зачета.

Текущий контроль успеваемости в форме защиты лабораторных и практических проводится в два этапа:

- 1-й этап: допуск к выполнению лабораторной работы – проводится в форме письменной «летучки» (5-10 мин) с целью контроля знаний студентов теоретической части лабораторной работы и готовности к выполнению практических исследований;

- 2-й этап выполняется по окончании каждой лабораторной работы (практического занятия) в форме индивидуального собеседования по выполненным исследованиям или расчетам. Проводится с целью контроля закрепления теоретической части материала и степени отработки студентом практических навыков исследования на аппаратуре.

Контрольные работы выполняются в виде короткого письменного ответа на один вопрос, изученный на предыдущей лекции в начале каждой последующей лекции. Ответ на вопрос дается в течение 5-10 минут. Таким образом, после лекционного курса каждого модуля формируется общая оценка за теоретические знания.

С целью повышения качества обучения за счет побуждения студентов к активной текущей учебной работе, четкого и оперативного контроля всего хода учебного процесса, снижения роли случайных и субъективных факторов при оценивании учебной деятельности студентов в образовательном процессе реализована модульно-рейтинговая система.

Правила ее использования прописаны в «Положении об МРС».

Набранные обучающимся баллы в рамках текущего контроля переводятся в оценку на зачете в соответствии со следующей шкалой:

– «не зачтено» - от 0 до 40 от максимального количества баллов;

– «зачтено» - от 41 до 100 максимального количества баллов.

Соотношения максимального количества баллов, полученных студентом по блокам модулей, показаны в Таблице 2.1.

Таблица 2.1 - Распределение баллов по модулям дисциплины «Основы информационной безопасности»

Модуль	Всего баллов (Максимальное значение)	Теоретический блок (Контрольная работа)	Практический блок
Модуль 1	50	10	40
Модуль 2	50	10	40
Модуль - Зачет	100		

Теоретический блок оценивается по результатам контрольной работы. Практический блок оценивается по результатам выполнения лабораторных работ и заданий на практических занятиях.

На экзамене (зачете) производится оценка тех компетенций, которые должны быть в той или иной форме освоены в процессе изучения. Рекомендуется формировать вопросы в билетах таким образом, чтобы преподаватель смог оценить все компетенции данной дисциплины.

2.2 Методика проведения зачета в группах заочной формы обучения

Зачет по дисциплине «Основы информационной безопасности» у обучающихся заочной формы обучения проводится письменно по классической методике. Вопросы сгруппированы в билетах. В каждом билете содержится по 2-3 вопроса, скомпонованные таким образом, чтобы преподаватель смог оценить все компетенции данной дисциплины. Количество билетов должно быть не менее числа обучающихся в группе. Обучающиеся готовят устные ответы на вопросы.

3. Промежуточная аттестация

Промежуточная аттестация проводится в форме зачета.

Зачет проводится по расписанию экзаменационной сессии в устном виде. Количество вопросов в билете – 2. Объявление результатов производится в день зачета. Результаты аттестации заносятся в зачетную ведомость и зачетную книжку обучающегося.

Обучающиеся, не прошедшие промежуточную аттестацию по графику сессии, должны ликвидировать задолженность в установленном порядке.

Образец билета к зачету

	МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»	Утверждаю И.О. Зав. кафедрой «ИБ» _____ Жуковский А.Г. «____» _____ 20___ г.
Направление подготовки: ***11.03.02 Инфокоммуникационные технологии и системы связи*** Курсы: 3 Дисциплина: ***Основы информационной безопасности***		
Билет №1 1. Понятие и сущность защиты информации (ЗИ). Назначение ЗИ. Задачи ЗИ. Принципы организации ЗИ. 2. Компьютерные вирусы и механизмы борьбы с ними. Профилактика заражения вирусами компьютерных систем. «____» _____ 20__ г. И.О.заведующий кафедрой «ИБ» _____ Жуковский А.Г.		

Один комплект отпечатанных билетов к зачету, подписанных преподавателем кафедры и утвержденных заведующим кафедрой хранится у заведующего кафедрой, другой комплект – у преподавателя, ведущего дисциплину

4. Тестовые задания для проведения оценки сформированности компетенций (ОПК-3)

Тестовые задания позволяют оценить уровень сформированности компетенции ОПК-3.

Задания распределены по блокам в соответствии с уровнем сложности. Каждый блок содержит номер задания, и текст задания.

Базовый уровень (Блок А) содержит примерно 50 % заданий.

Он формируется из заданий с выбором одного или нескольких верных ответов из предложенных или воспроизведения фактического материала (терминология, факты, классификация, параметры и др.);

Повышенный уровень (Блок Б) в среднем составляет 35 % заданий.

В нем используются задания на сопоставление, сравнение, установление последовательности;

Высокий уровень (Блок В) в среднем составляют – 15 % заданий.

В задании используются: решения нетиповых задач, алгоритмы, доказательства, задания с развернутым ответом – определения, перечисление, изображение схемы, структуры и др.

Количество заданий по компетенции ОПК-3 равно 20.

Один комплект тестовых вопросов с указанием правильных ответов хранится у заведующего кафедрой, другой комплект – у преподавателя, ведущего дисциплину.

ОПК-3. Способен применять методы поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности.

БЛОК А (базовый уровень) – Задание с выбором одного или нескольких верных ответов из предложенных

Инструкция по тестам Блока А: Прочитайте текст и выберите один или несколько правильных ответов

№	Дисциплина	Тексты заданий
1	Б1.О.24 «Основы информационной безопасности»	**К правовым методам, обеспечивающим информационную безопасность, относятся:** 1. Разработка аппаратных средств 2. Разработка и установка во всех компьютерных сетях сетевых фильтров. 3. Разработка и конкретизация нормативных актов обеспечения безопасности
2	Б1.О.24 «Основы информационной безопасности»	**Основные объекты информационной безопасности:** 1. Вычислительные системы, компьютерные сети, базы данных 2. Информационные системы, психологическое состояние пользователей 3. Бизнес-ориентированные, коммерческие системы
3	Б1.О.24 «Основы информационной безопасности»	**Основными рисками информационной безопасности являются:** 1. Искажение, уменьшение объема, перекодировка информации 2. Техническое вмешательство, выведение из строя оборудования сети 3. Потеря, искажение, утечка информации
4	Б1.О.24 «Основы информационной безопасности»	**Антивирус полностью защищает компьютер от вирусов и атак при работе в сети. Вы согласны с этим**? 1. Нет 2. Да, если это лицензионный антивирус известного производителя 3. Защищает совместно с включенным брандмауэром 4. Да
5	Б1.О.24 «Основы информационной безопасности»	**Основными субъектами информационной безопасности являются:** 1. Руководители, менеджеры, администраторы компаний 2. Органы права, государства, бизнеса 3. Сетевые базы данных, файерволы
6	Б1.О.24 «Основы информационной безопасности»	**Принципом политики информационной безопасности является принцип:** 1. Невозможности миновать защитные средства сети (системы) 2. Усиления основного звена сети, системы 3. Полного блокирования доступа при риск-ситуациях
7	Б1.О.24 «Основы информационной безопасности»	**Когда получен спам по e-mail с приложенным файлом, следует:** 1. Прочитать приложение, если оно не содержит ничего ценного – удалить 2. Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама

№	Дисциплина	Тексты заданий
		3. Удалить письмо с приложением, не раскрывая (не читая) его
8	Б1.О.24 «Основы информационной безопасности»	**Угроза информационной системе (компьютерной сети) – это:** 1. Вероятностное событие 2. Детерминированное (всегда определенное) событие 3. Событие, происходящее периодически
9	Б1.О.24 «Основы информационной безопасности»	**Очень сложные пароли гарантируют 100% защиту?** 1. Нет 2. Да, если после работы полностью очищать куки и не хранить пароль на компьютере 3. Да, если пароль не сохранен на компьютере
10	Б1.О.24 «Основы информационной безопасности»	**Какие вирусы активизируются после включения компьютера?** 1. Снифферы 2. Загрузочные 3. Трояны 4. Черви

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление соответствия

Инструкция: Прочитайте текст и установите соответствие

№	Дисциплины	Тексты заданий
11	Б1.О.24 «Основы информационной безопасности»	**Установите соответствие вредоносных воздействий их определениям:** 1. Троян 2. Бэкдор 3. Вирус 4. Эксплойт А. Компьютерная программа, фрагмент программного кода или последовательность команд, которые используют уязвимости в программном обеспечении для атаки на вычислительную систему Б. Дефект алгоритма, который намеренно встраивается в него разработчиком / злоумышленником и позволяет получить несанкционированный доступ к данным или удалённому управлению операционной системой В. Вид вредоносного программного обеспечения, который маскируется под легальное ПО Г. Вид вредоносных программ, способных внедряться в код других программ, системные области памяти, загрузочные секторы и распространять свои копии по разнообразным каналам связи
12	Б1.О.24 «Основы информационной безопасности»	**Установите соответствие систем их назначению:** 1. DLP (Data Loss Prevention) 2. IRP (Incident Response Platform) 3. SIEM (Security Information and Event Management) 4. SOC (Security Operations Center) 5. Deception. А. Централизованная система управления ложными сетевыми объектами, которые принято называть ловушками Б. Центр мониторинга и реагирования на инциденты информационной безопасности. Специальное подразделение, которое круглосуточно следит за IT-инфраструктурой компании В. Система управления информационной безопасностью и событиями безопасности Г. Платформа реагирования на инциденты Д. Система предотвращения утечек информации
13	Б1.О.24 «Основы информационной безопасности»	**Установите соответствие специализированного ПО его назначению:** 1. ESET NOD32 2. Steganos Privacy Suite 3. Handy Recovery 4. Information Backup System А. Программное обеспечение по резервному копированию данных Б. Антивирусное ПО В. Программное обеспечение по шифрованию информации Г. Программное обеспечение по восстановлению данных.
14	Б1.О.24 «Основы информационной безопасности»	**Установите соответствие направления информационной безопасности соответствующим мероприятиям:** 1. Правовая защита

№	Дисциплины	Тексты заданий
		2. Организационная защита 3. Инженерно-техническая защита А. Установка кодовых замков на дверях. Б. Разработка локальных нормативных актов. В. Подбор сотрудников для работы в службе информационной безопасности.

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление последовательности

Инструкция: Прочитайте текст и установите правильную последовательность

№	Дисциплина	Тексты заданий
15	Б1.О.24 «Основы информационной безопасности»	**Расставьте в порядке значимости нормативные акты, регламентирующие вопросы информационной безопасности:** 1. Локальные нормативные акты 2. Приказы соответствующих Министерств и Ведомств 3. Законы РФ 4. Указы Президента РФ 5. Конституция РФ 6. Постановления Правительства РФ
16	Б1.О.24 «Основы информационной безопасности»	**Установите правильный порядок установки ПО на рабочую станцию:** 1. Установка драйверов 2. Установка операционной системы 3. Обновление прошивки BIOS 4. Установка прикладного и специального ПО 5. Установка антивируса 6. Установка обновления операционной системы
17	Б1.О.24 «Основы информационной безопасности»	**Расставьте в порядке возрастания вероятности различного вида угроз:** 1. Кража оборудования 2. Кража информации сотрудниками 3. Вредоносные программы.

БЛОК В (высокий уровень) – Задание открытого типа с развернутым ответом

Инструкция: Прочитайте текст и запишите ответ

№	Дисциплина	Тексты заданий
18	Б1.О.24 «Основы информационной безопасности»	**Вставьте пропущенное слово:** Ознакомление с информацией, обработка или уничтожение информации – это _____ к информации**.**
19	Б1.О.24 «Основы информационной безопасности»	**Вставьте пропущенное слово:** Единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа – это _____ доступа**.**
20	Б1.О.24 «Основы информационной безопасности»	**Напишите название термина:** Комплекс мер, направленных на защиту компьютерных систем, сетей и данных от несанкционированного доступа, использования, раскрытия, уничтожения или изменения – это _____.

Система оценивания выполнения тестовых заданий по компетенции ОПК-3, формируемой дисциплиной «Основы информационной безопасности»

Номер задания	Указания по оцениванию	Результат оценивания (баллы, полученные за выполнение задания/характеристика правильности ответа)
Задания 1-10	Задания с выбором одного или нескольких верных ответов из предложенных считается верным, если	Совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие

	правильно указана цифра или цифры, означающие верные ответы.	- 0 баллов.
Задания 11-14	Задания закрытого типа на установление соответствия считается верным, если правильно установлены все соответствия (позиции из одного столбца верно сопоставлены с позициями другого)	Полное совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 15-17	Задания закрытого типа на установление последовательности считается верным, если правильно указана вся последовательность цифр	Полное совпадение с верным ответом оценивается 1 баллом; если допущены ошибки или ответ отсутствует- 0 баллов.
Задания 18-20	Задание открытого типа с развернутым ответом считается верным, если ответ совпадает с эталонным по содержанию и полноте.	Полный правильный ответ на задание оценивается 1 баллом. Если в ответе используются перечисления, то различный порядок следования правильных ответов в перечислении не считается ошибкой. Если допущена ошибка, ответ не полный, неправильный или отсутствует - 0 баллов.

Приложение 2

Методические рекомендации по освоению дисциплины

1. Методические рекомендации преподавателю

Дисциплина «Основы информационной безопасности» включает в себя:

- лекционные занятия;
- практические занятия;
- промежуточную аттестацию – зачет.

Перед началом изучения дисциплины преподаватель должен ознакомить студентов с рабочей программой и оценочными материалами по дисциплине, с видами учебной и самостоятельной работы, перечнем литературы и интернет-ресурсов, с формами текущей и промежуточной аттестации, с критериями оценки качества знаний для итоговой оценки по дисциплине.

При проведении лекций, преподаватель:

1) формулирует тему и цель занятия, объявляет учебные вопросы;

2) излагает основные теоретические положения;

3) с помощью технических средств обучения и/или под запись дает определения основных понятий, расчетных формул;

4) проводит примеры из отечественного и зарубежного опыта, дает текущие статистические данные для наглядного и образного представления изучаемого материала;

5) в конце занятия выдает вопросы для самостоятельного изучения.

На занятиях лабораторного цикла следует обратить внимание на соответствие выбираемых студентом средств выполнения решаемым в работе задачам.

Каждая лабораторная работа должна быть оформлена и защищена в соответствии с требованиями. Защита производится после оформления отчета по работе.

Во время выполнения заданий в учебной аудитории студент может консультироваться с преподавателем, определять наиболее эффективные методы решения поставленных задач. Если какая-то часть задания остается не выполненной, студент может продолжить её выполнение во время внеаудиторной самостоятельной работы.

Для оценки полученных знаний и освоения учебного материала по каждому разделу и в целом по дисциплине преподаватель использует формы текущего, промежуточного и итогового контроля знаний обучающихся.

2. Методические рекомендации обучающимся

Приступая к изучению новой учебной дисциплины, студенты должны ознакомиться с рабочей программой, оценочными материалами, учебной, научной и методической литературой, имеющейся в ЭИОС СКФ МТУСИ,

Глубина усвоения дисциплины зависит от активной и систематической работы студента на лекциях и практических занятиях, а также в ходе самостоятельной работы, по изучению рекомендованной литературы.

2.1 Методические указания для обучающихся по лекционным занятиям

Важно сосредоточить внимание на содержании лекции. Это поможет лучше воспринимать учебный материал и уяснить взаимосвязь проблем по всей дисциплине.

Основное содержание лекции целесообразнее записывать в тетради в виде ключевых фраз, понятий, тезисов, обобщений, схем, опорных выводов. Необходимо обращать внимание на термины, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации. Желательно оставлять в конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющей материал

прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

С целью уяснения теоретических положений, разрешения спорных ситуаций необходимо задавать преподавателю уточняющие вопросы. Для закрепления содержания лекции в памяти, необходимо во время самостоятельной работы внимательно прочесть свой конспект и дополнить его записями из учебников и рекомендованной литературы.

Конспектирование читаемых лекций и их последующая доработка способствует более глубокому усвоению знаний, и поэтому являются важной формой учебной деятельности студентов.

2.2 Методические указания для обучающихся по подготовке к практическим занятиям

Целью практических занятий является закрепление теоретических знаний, полученных при изучении дисциплины.

При подготовке к практическому занятию целесообразно выполнить следующие рекомендации:

- изучить основную литературу; ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях: журналах, газетах и т.д.;
- при необходимости доработать конспект лекций. При этом учесть рекомендации преподавателя и требования учебной программы.

При выполнении практических занятий основным методом обучения является самостоятельная работа студента под управлением преподавателя. На них пополняются теоретические знания студентов, их умение творчески мыслить, анализировать, обобщать изученный материал, проверяется отношение студентов к будущей профессиональной деятельности.

Оценка выполненной работы осуществляется преподавателем комплексно: по результатам выполнения заданий, устному сообщению и оформлению работы.

После подведения итогов занятия студент обязан устранить недостатки, отмеченные преподавателем при оценке его работы.

3. Методические рекомендации для обучающихся по самостоятельной работе

Самостоятельная работа студентов является составной частью учебной работы и имеет целью закрепление и углубление полученных знаний и навыков, поиск и приобретение новых знаний, в том числе с использованием автоматизированных обучающих курсов (систем), а также выполнение учебных заданий, подготовку к предстоящим занятиям, зачетам и экзаменам.

Самостоятельная работа во внеаудиторное время включает в себя:

- повторение лекционного материала;
- подготовки к лабораторным работам (практическим занятиям);
- изучения учебной и научной литературы;
- решения задач, выданных на практических занятиях;
- подготовки к тестированию;
- выделение наиболее сложных и проблемных вопросов по изучаемой теме, получение разъяснений и рекомендаций по данным вопросам с преподавателями кафедры на их еженедельных консультациях.
- проведение самоконтроля путем ответов на вопросы текущего контроля знаний, решения представленных в учебно-методических материалах кафедры задач, тестов, написания рефератов по отдельным вопросам изучаемой дисциплины.

Самостоятельная работа организуется преподавателями, обеспечивается и контролируется кафедрами. Она предусматривает, как правило, разработку рефератов, выполнение расчетно-графических, вычислительных работ, моделирования и других творческих заданий в соответствии с учебной программой (тематическим планом изучения дисциплины). Основная

цель данного вида занятий состоит в обучении курсантов методам самостоятельной работы с учебным материалом.

Материал, подлежащий обработке на самостоятельных занятиях, намечается при разработке программы самостоятельной работы. Опыт, накопленный кафедрами в организации самостоятельных занятий, что материал выделяемый на такие занятия, должен удовлетворять следующим требованиям:

- быть изложенным в учебнике достаточно полно и с примерами;
- обеспечиваться достаточным количеством литературы, учебных пособий. учебно-методических материалов, образцов техники
- содержать материал, углубляющий знания, полученные на лекции;
- осваивать проблемные еще не полностью решенные вопросы.

Перед выполнением внеаудиторной самостоятельной работы преподаватель проводит инструктаж (консультацию) с определением цели задания, его содержания, сроков выполнения, основных требований к результатам работы, критериев оценки, форм контроля и перечня источников и литературы.

Обычно постановку задачи обучающимся на проведение самостоятельной работы преподаватель осуществляет на одном из занятии, предшествующему данному.

Методику самостоятельной работы все обучающиеся выбирают индивидуально.

Обучающимся очной/заочной/очно-заочной форм(мы) обучения при освоении вопросов для самостоятельного изучения, представленных в подразделе(лах) 4.1/4.2/4.3 рабочей программы, рекомендуется соблюдать последовательность их изучения, представленную, соответственно, в таблице1/таблице 2/таблице 3.

Таблица 1. – Учебный материал, выносимый на самостоятельное изучение студентам очной формы обучения

№	Темы, разделы, вынесенные на самостоятельную подготовку, вопросы для подготовки к практическим и лабораторным занятиям; курсовые работы, содержание контрольных работ; рекомендации по использованию литературы, ЭВМ и др.	Часов всего: 40
	Модуль 1 – 20 часов	
1	Алгоритм симметричной системы шифрования данных – стандарт ГОСТ 28147-89	2
2	Алгоритм ассиметричной (двухключевой) системы шифрования данных RSA;	2
3	Гостехкомиссия России. Руководящий документ Защита от несанкционированного доступа к информации. Термины и Определения;	2
4	Доктрина информационной безопасности Российской Федерации;	2
5	Указ президента российской федерации. Об утверждении перечня сведений конфиденциального характера;	2
6	Положение о лицензировании деятельности по технической защите конфиденциальной информации. Постановление Правительства Российской Федерации от 30 апреля 2002 г. № 290.	4
7	Инструкция по защите конфиденциальной информации при работе с зарубежными партнерами.	2
8	Обеспечение сохранения коммерческой тайны предприятия. Каталог обобщенных мероприятий по защите конфиденциальной информации.	4
	Модуль 2 – 20 часов	
9	Анализ структуры и принципов функционирования вычислительных сетей с позиции обеспечения информационной безопасности.	2
10	Угрозы информационно-программному обеспечению, характерные только для распределённой вычислительной среды.	2
11	Классификация компьютерных вирусов	2
12	Методы и средства борьбы с вирусами	2
13	Профилактика заражения вирусами компьютерных систем.	2

14	Порядок действий пользователя при обнаружении заражения ЭВМ вирусами	2
15	Анализ моделей нарушителя; угрозы информационно-программному обеспечению вычислительных систем и их классификация.	4
16	Основные способы защиты от потери информации и нарушений работоспособности сетей и систем; внесение функциональной и информационной избыточности; способы резервирования информации; правила обновления резервных данных.	4

Таблица 2. – Учебный материал, выносимый на самостоятельное изучение студентам заочной формы обучения

№	Темы, разделы, вынесенные на самостоятельную подготовку, вопросы для подготовки к практическим и лабораторным занятиям; курсовые работы, содержание контрольных работ; рекомендации по использованию литературы, ЭВМ и др.	Часов всего: 60
	Модуль 1 – 34 часа	
1	Направления обеспечения информационной безопасности	4
2	Защита информации от утечки по техническим каналам	4
3	Исследование характеристик и возможностей программ по защите и сокрытию файлов, папок	4
4	Исследование характеристик и возможностей программ по шифрованию, безвозвратному удалению, стеганографии	4
5	Алгоритм симметричной системы шифрования данных – стандарт ГОСТ 28147-89	4
6	Алгоритм ассиметричной (двухключевой) системы шифрования данных RSA;	2
7	Гостехкомиссия России. Руководящий документ Защита от несанкционированного доступа к информации. Термины и Определения;	2
8	Доктрина информационной безопасности Российской Федерации;	2
9	Указ президента российской федерации. Об утверждении перечня сведений конфиденциального характера;	2
10	Положение о лицензировании деятельности по технической защите конфиденциальной информации. Постановление Правительства Российской Федерации от 30 апреля 2002 г. № 290.	2
11	Инструкция по защите конфиденциальной информации при работе с зарубежными партнерами.	2
12	Обеспечение сохранения коммерческой тайны предприятия. Каталог обобщенных мероприятий по защите конфиденциальной информации.	2
	Модуль 2 – 26 часов	
13	Классификация методов криптографического преобразования информации Шифрование. Основные понятия Методы шифрования с симметричным ключом Системы шифрования с открытым ключом Стандарты шифрования Перспективы использования криптозащиты информации в КС.	6
14	Проблемы обеспечения безопасности обработки и хранения информации в вычислительных системах. Базовые этапы построения системы комплексной защиты вычислительных систем. Анализ моделей нарушителя; угрозы информационно-программному обеспечению. Исследование характеристик и возможностей антивирусного ПО	4
15	Анализ структуры и принципов функционирования вычислительных сетей с позиции обеспечения информационной безопасности.	2

16	Угрозы информационно-программному обеспечению, характерные только для распределённой вычислительной среды.	2
17	Классификация компьютерных вирусов	2
18	Методы и средства борьбы с вирусами	2
19	Профилактика заражения вирусами компьютерных систем.	2
20	Порядок действий пользователя при обнаружении заражения ЭВМ вирусами	2
21	Анализ моделей нарушителя; угрозы информационно-программному обеспечению вычислительных систем и их классификация.	2
22	Основные способы защиты от потери информации и нарушений работоспособности сетей и систем; внесение функциональной и информационной избыточности; способы резервирования информации; правила обновления резервных данных.	2

Таблица 3 – Учебный материал, выносимый на самостоятельное изучение студентам очно-заочной формы обучения

№	Темы, разделы, вынесенные на самостоятельную подготовку, вопросы для подготовки к практическим и лабораторным занятиям; курсовые работы, содержание контрольных работ; рекомендации по использованию литературы, ЭВМ и др.	Часов всего: 60
	Модуль 1 – 30 часов	
1	Правовая защита Организационная защита Инженерно-техническая защита	4
2	Направления обеспечения информационной безопасности Защита информации от утечки по техническим каналам	4
3	Исследование характеристик и возможностей программ по защите и сокрытию файлов, папок	2
4	Исследование характеристик и возможностей программ по шифрованию, безвозвратному удалению, стеганографии	2
5	DLP-системы	2
6	Алгоритм симметричной системы шифрования данных – стандарт ГОСТ 28147-89	2
7	Алгоритм ассиметричной (двухключевой) системы шифрования данных RSA;	2
8	Гостехкомиссия России. Руководящий документ Защита от несанкционированного доступа к информации. Термины и Определения;	2
9	Доктрина информационной безопасности Российской Федерации;	2
10	Указ президента российской федерации. Об утверждении перечня сведений конфиденциального характера;	2
11	Положение о лицензировании деятельности по технической защите конфиденциальной информации. Постановление Правительства Российской Федерации от 30 апреля 2002 г. № 290.	2
12	Инструкция по защите конфиденциальной информации при работе с зарубежными партнерами.	2
13	Обеспечение сохранения коммерческой тайны предприятия. Каталог обобщенных мероприятий по защите конфиденциальной информации.	2
	Модуль 2 – 30 часов	
14	Исследование характеристик и возможностей антивирусного ПО	4
15	Криптографические методы защиты информации	2
16	Структура и принципы функционирования современных вычислительных систем.	2
17	Проблемы обеспечения безопасности обработки и хранения информации в вычислительных системах.	2
18	Базовые этапы построения системы комплексной защиты вычислительных систем.	2

19	Анализ моделей нарушителя; угрозы информационно-программному обеспечению.	2
20	Анализ структуры и принципов функционирования вычислительных сетей с позиции обеспечения информационной безопасности.	2
21	Угрозы информационно-программному обеспечению, характерные только для распределённой вычислительной среды.	2
22	Классификация компьютерных вирусов	2
23	Методы и средства борьбы с вирусами	2
24	Профилактика заражения вирусами компьютерных систем.	2
25	Порядок действий пользователя при обнаружении заражения ЭВМ вирусами	2
26	Анализ моделей нарушителя; угрозы информационно-программному обеспечению вычислительных систем и их классификация.	2
27	Основные способы защиты от потери информации и нарушений работоспособности сетей и систем; внесение функциональной и информационной избыточности; способы резервирования информации; правила обновления резервных данных.	2

Самостоятельная работа обучающихся над усвоением материала по дисциплине может выполняться в помещении для самостоятельной работы СКФ МТУСИ, посредством использования электронной библиотеки и ЭИОС.