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 УВР
_____ Жуковский А.Г.
«30» 12 2022 г.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
по дисциплине
Основы информационной безопасности сетей и систем Б1.О.25

Кафедра: Инфокоммуникационные технологии и системы связи
Направление подготовки: **11.03.02 Инфокоммуникационные технологии и системы связи**
Профиль **Защищенные инфокоммуникационные системы**
Мобильная связь и интернет вещей
Инфокоммуникационные системы и сети
Формы обучения: **очная, очно-заочная, заочная**
Разработал:
Профессор кафедры ИТСС, д.п.н., доцент Жуковский А.Г.
Рецензент(ы):
Ведущий сотрудник ФГУП «РНИИРС, д.т.н., доцент Елисеев А.В.

Разработаны в соответствии с ФГОС ВО:
Федеральным государственным образовательным стандартом высшего образования, направление подготовки 11.03.02 ИНФОКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ СВЯЗИ, утвержденным приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 г. N 930.

Составлены на основании учебных планов
направления 11.03.02 Инфокоммуникационные технологии и системы связи профилей «Защищенные инфокоммуникационные системы», «Мобильная связь и интернет вещей», «Инфокоммуникационные системы и сети», одобренных Учёным советом СКФ МТУСИ, протокол № 5 от 26.12.2022, и утвержденных директором СКФ МТУСИ 26.12.2022г.

Рассмотрены и одобрены на заседании кафедры
«Инфокоммуникационные технологии и системы связи»

Протокол от «19» 12 2022г. № 5

Зав. кафедрой _____ Юхнов В.И.

Визирование для использования в 20__/20__ уч. году

Утверждаю

Зам. директора по УВР ________________
«___» __________ 20__ г.

Обновление ОМ обсуждено и одобрено на заседании кафедры
«Инфокоммуникационные технологии и системы связи»

Протокол от «___» _______ 20__ г. № ____

Зав. кафедрой ______________________

Визирование для использования в 20__/20__ уч. году

Утверждаю

Зам. директора по УВР ____________________
«___» __________ 20__ г.

Обновление ОМ обсуждено и одобрено на заседании кафедры
«Инфокоммуникационные технологии и системы связи»

Протокол от «___» _______ 20__ г. № ____

Зав. кафедрой ______________________

Визирование для использования в 20__/20__ уч. году

Утверждаю

Зам. директора по УВР ________________
«___» __________ 20__ г.

Обновление ОМ обсуждено и одобрено на заседании кафедры
«Инфокоммуникационные технологии и системы связи»

Протокол от «___» _______ 20__ г. № ____

Зав. кафедрой ______________________

Визирование для использования в 20__/20__ уч. году

Утверждаю

Зам. директора по УВР ________________
«___» __________ 20__ г.

Обновление ОМ обсуждено и одобрено на заседании кафедры
«Инфокоммуникационные технологии и системы связи»

Протокол от «___» _______ 20__ г. № ____

Зав. кафедрой ______________________

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
УК-2		
Знать:		
опасности и угрозы, возникающие в развитии современного информационного общества, основные требования информационной безопасности	Контрольная работа	Модуль 1 0÷5 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5
Уметь		
Защищать интеллектуальную собственность средствами патентного и авторского права; правовая регламентация охранной деятельности	Практическое занятие 1-3	Модуль 1 0÷12 «Удовлетворительно» - 5-7 «Хорошо» - 8-10 «Отлично» - 11-12
Владеть		
Средства и методы физической защиты объектов; системы сигнализации, видеонаблюдения, контроля доступа	Лабораторная работа 1-2	Модуль 1 0÷8 «Удовлетворительно» - 3-4 «Хорошо» - 5-6 «Отлично» - 7-8
ОПК-3		
Знать:		
Основы информационной и библиографической культуры, основные требования информационной безопасности	Контрольная работа	Модуль 1 0÷5 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5

Уметь:		
Решать задачи профессиональной деятельности на основе информационной и библиографической культуры с применением инфокоммуникационных технологий и с учетом основных требований информационной безопасности	Практическое занятие 1-3	Модуль 1 0÷12 «Удовлетворительно» - 5-7 «Хорошо» - 8-10 «Отлично» - 11-12
Владеть:		
Алгоритмом симметричной системы шифрования данных – стандарт ГОСТ 28147-89».	Лабораторная работа 1-2	Модуль 1 0÷8 «Удовлетворительно» - 3-4 «Хорошо» - 5-6 «Отлично» - 7-8
УК-2		
Знать		
Представление защищаемой информации; угрозы безопасности информации; ценность информации; основные термины и понятия криптографии;	Контрольная работа	Модуль 2 0÷5 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5
Уметь		
Использовать криптографические методы для защиты данных, циркулирующих в вычислительной сети	Лабораторная работа 3-4	Модуль 2 0÷10 «Удовлетворительно» - 4-6 «Хорошо» - 7-8 «Отлично» - 9-10
Владеть		
Алгоритмом электронной цифровой подписи на основе криптосистемы RSA	Лабораторная работа 5-6	Модуль 2 0÷10 «Удовлетворительно» - 3-5 «Хорошо» - 6-8 «Отлично» - 9-10
ОПК-3		
Знать		
Открытые сообщения и их характеристики; модели открытых сообщений; исторический очерк развития криптографии; типы криптографических систем; простые методы шифрования; шифры подстановки и перестановки	Контрольная работа	Модуль 2 0÷5 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5
Уметь		
Концептуальные вопросы построения уровней защиты систем управления базами данных (СУБД)	Лабораторная работа 3-4	Модуль 2 0÷10 «Удовлетворительно» - 3-5

		«Хорошо» - 6-8 «Отлично» - 9-10
Владеть		
Стандартами по оценке уровня безопасности ОС; внесение функциональной и информационной избыточности ресурсов на уровне ОС	Лабораторная работа 5-6	Модуль 2 0÷10 «Удовлетворительно» - 3-5 «Хорошо» - 6-8 «Отлично» - 9-10
Экзамен		«Удовлетворительно» - 41-60 «Хорошо» - 61-80 «Отлично» - 81-100

1.3 Оценочные материалы: типовые контрольные задания, иные материалы

1.3.1 Оценочные средства для очной формы обучения

Модуль 1 (50 баллов):

Модуль содержит 4 лекционных занятий, 3 практических занятия и 2 лабораторные работы. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 10. За выполненные и защищенные практические занятия студент получает максимум 24 балла. За выполненные и защищенные лабораторные работы студент получает максимум 16 баллов. Общее максимальное количество баллов за модуль 1 составляет 50.

Вопросы для контрольной работы (УК-2, 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.

Правовая защита от компьютерных преступлений и защита интеллектуальной собственности.

Контрольные вопросы ПЗ№1 (УК-2, ОПК-3):

1. Назовите особенности расследования компьютерных преступлений.
2. Какие задачи решаются судебно-бухгалтерской и программно-технической экспертизами при проведении следственных действий?
3. Существующая классификация компьютерных преступлений. Методы НСД.
4. Методы и приемы предупреждения компьютерных преступлений. Анализ компьютерных преступлений.
5. В каких документах представлены нормы правового обеспечения защиты информации в АС?
6. Что представляет собой документ «Политика безопасности»?
7. Какие документы необходимо представить для присвоения класса защищенности АС?
8. Выполнение каких правил безопасности обеспечивается путем реализации «Политики безопасности»?
9. Где указаны требования к безопасности компьютерных сетей в РФ?
10. Международные соглашения в информационной сфере.
11. Назовите правовые формы охраны интеллектуальной собственности.
12. Что понимается под исключительными правами на объекты интеллектуальной собственности?
13. Правовая охрана авторских смежных прав.
14. Правовая охрана программ для ЭВМ и баз данных.
15. Правовая охрана объектов промышленной собственности.
16. Охрана исключительного права на секрет производства.
17. Правовая защита фирменного наименования, товарных знаков, знаков обслуживания и наименования мест происхождения товаров.

Практическое занятие №2. Противодействие несанкционированному доступу к источникам конфиденциальной информации

Контрольные вопросы ПЗ№2 (УК-2, ОПК-3):

1. Способы несанкционированного доступа

2. Технические средства несанкционированного доступа к информации

3. Защита от наблюдения и фотографирования

4. Защита от подслушивания

5. Противодействие незаконному подключению к линиям связи

6. Защита от перехвата.

Практическое занятие №3 Технические средства обеспечения информационной безопасности

1. Поисковое оборудование.

2. Технические средства активного и пассивного противодействия нарушениям информационной безопасности.

Контрольные вопросы ПЗ№3 (УК-2, ОПК-3):

1. Против каких видов утечки информации служит обнаружитель скрытых видеокамер?

2. Для чего нужен панорамный индикатор поля?

3. Для чего нужен панорамный селективный поля?

4. Что такое ПЭМИН?

5. Назовите акустические каналы утечки информации.

6. Назовите каналы электромагнитной утечки информации.

7. С какой целью проводится анализ сигналов?.

8. Какие устройства могут относиться к электронным устройствам негласного получения информации (ЭУНПИ)?

9. Какими функциями обладают анализаторы спектра?

10. С какой целью необходимо подавлять Wi-Fi и другие беспроводные сети связи?

11. Какая информация определяется при проведении радиомониторинга?

12. В какой полосе частот могут функционировать анализаторы радиочастотного спектра?

13. Как может быть осуществлена модуляция голосовой информации (примеры)?

14. Что могут обнаружить системы рентгеновского контроля?

15. Что может обнаруживать нелинейный локатор?

16. В каких случаях применяется нелинейный локатор и в каких – анализатор радиочастотного спектра?

17. Какой принцип противодействия используется в подавителях диктофонов и микрофонов?

18. Какие функции выполняют сетевые фильтры?

19. Какую функцию выполняет акустический сейф?

20. С какой целью на стекла окон устанавливаются вибровозбудители?

21. Какие существуют разновидности генераторов шума?

22. Какой материал используется в экранирующих устройствах?

23. Для чего используются безэховые акустические камеры?

24. Для каких целей используются компьютеры и множительные устройства в защищенно исполнении?

25. Какие параметры измеряются в системах радиомониторинга?

26. Перечислите программные средства, которые могут использоваться для обеспечения информационной безопасности.

Лабораторная работа 1. Исследование характеристик и возможностей программ по защите и сокрытию файлов, папок

Контрольные вопросы ЛР№1 (УК-2, 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

Лабораторная работа 2. Исследование характеристик и возможностей программ по шифрованию, безвозвратному удалению, стеганографии

Контрольные вопросы ЛР№2 (УК-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

Модуль 2: (50 баллов):

Модуль содержит 3 лекционных занятия и 4 лабораторных работы. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 10. За выполненные и защищенные лабораторные работы студент получает максимум 40 баллов. Общее максимальное количество баллов за модуль 2 составляет 50.

Вопросы для контрольной работы (УК-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

Лабораторная работа 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 ЛР№3 (УК-2, 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.

Лабораторная работа 4. Исследование характеристик и возможностей антивирусного ПО

Контрольные вопросы ЛР№4 (УК-2, 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

Лабораторная работа 5. Исследование характеристик и возможностей программ по восстановлению потерянных данных

Контрольные вопросы ЛР№5 (УК-2, 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

Лабораторная работа 6. Исследование характеристик и возможностей программ по организации резервного копирования

Контрольные вопросы ЛР№6 (УК-2, 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 экзамен по дисциплине «Основы информационной безопасности сетей и систем»

1. Понятие и сущность ЗИ. Назначение ЗИ. Задачи ЗИ. (УК-2)
2. Методологические основы организации ЗИ. (УК-2)
3. Принципы организации ЗИ. Основные требования, предъявляемые к ЗИ. (УК-2)
4. Правовое регулирование в области безопасности информации. (УК-2)
5. Общая характеристика организационных методов защиты информации. (УК-2)
6. Основные факторы, влияющие на организацию ЗИ. (УК-2)
7. Функции руководства предприятия и подразделений предприятия, экспертной комиссии, службы защиты информации. (УК-2)
8. Классификация информации по видам тайны и степеням конфиденциальности. Нормативное закрепление состава защищаемой информации; структура перечней сведений, относимых к различным видам тайны. (УК-2)

9. Значение носителей защищаемой информации как объектов защиты. Факторы, определяющие состав носителей информации. (УК-2)
10. Методика выявления состава носителей защищаемой информации. Хранилища носителей информации как объект защиты. (УК-2)
11. Особенности помещений для работы с защищаемой информацией как объектов защиты. (УК-2)
12. Состав технических средств обработки, передачи, транспортировки и защиты информации, являющихся объектами защиты. (УК-2)
13. Определение возможных методов несанкционированного доступа к защищаемой информации. (УК-2)
14. Методика выявления нарушителей (незаконных пользователей) и состава интересующей их информации. (УК-2)
15. Факторы, влияющие на выбор компонентов КСЗИ. Объекты защиты как основной фактор, определяющий состав компонентов КСЗИ. (УК-2)
16. Обеспечение полноты составляющих защиты. Учет всех факторов и обстоятельств, оказывающих влияние на качество защиты. (УК-2)
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. (УК-2)
18. Понятие модели объекта, основные виды моделей и их характеристика. (УК-2)
19. Распределение функций по защите информации между руководством предприятия, службой защиты информации, специальными комиссиями и пользователями защищаемой информации, обеспечение взаимодействия между ними. (УК-2)
20. Разработка нормативных документов, регламентирующих деятельность персонала по защите информации. Подбор и обучение персонала. (УК-2)
21. Состав нормативно-методических документов по обеспечению функционирования КСЗИ, их назначение, структура и содержание. Порядок разработки и внедрения документов. (УК-2)
22. Содержание и особенности экспертной оценки эффективности защиты. (УК-2)
23. Сведения, составляющие коммерческую тайну предприятия (УК-2)
24. Порядок ведения делопроизводства документов, содержащих коммерческую тайну (УК-2)
25. Угрозы безопасности информации в компьютерных системах. (УК-2)
26. Угрозы для протоколов и служб Internet (УК-2)
27. Виртуальные частные сети и их информационная защита (ОПК-3)
28. Методы идентификации и аутентификации пользователей (ОПК-3)
29. Инструментальные средства тестирования системы защиты (ОПК-3)
30. Межсетевые экраны (ОПК-3)
31. Оценка защищенности информации от утечки по каналам ПЭМИН (ОПК-3)
32. Управление защитой информации в распределенных сетях (ОПК-3)

33. Основные концептуальные положения системы защиты информации (ОПК-3)
34. Действия, приводящие к неправомерному овладению конфиденциальной информацией (ОПК-3)
35. Направления обеспечения безопасности (УК-2)
36. Правовые документы по защите информации и их характеристика (УК-2)
37. Задачи по обеспечению организационных мероприятий по защите информации. (УК-2)
38. Классификация мер инженерно-технической защиты информации. (ОПК-3)
39. Классификация инженерно-технической защиты информации по техническим средствам. (ОПК-3)
40. Классификация программных средств защиты информации(ОПК-3)
41. Каналы разглашения конфиденциальной информации. (ОПК-3)
42. Способы пресечения разглашения информации. (ОПК-3)
43. Каналы утечки конфиденциальной информации. Их классификация. (ОПК-3)
44. Защита информации от утечки по визуально-оптическим каналам (ОПК-3)
45. Защита информации от утечки но акустическим каналам (ОПК-3)
46. Защита информации от утечки по электромагнитным каналам (ОПК-3)
47. Способы несанкционированного доступа (ОПК-3)
48. Защита от наблюдения и фотографирования (ОПК-3)
49. Способы прослушивания посредством радиозакладок. (ОПК-3)
50. Обеспечение безопасности телефонных переговоров (ОПК-3)
51. Назначение и характеристики нелинейных локаторов (ОПК-3)
52. Назначение и характеристики средств постановки активных помех (ОПК-3)
53. Назначение и принцип работы скремблеров (дескремблеров) (ОПК-3)
54. Противодействие незаконному подключению к линиям связи (ОПК-3)
55. Меры защиты от радиоперехвата (ОПК-3)
56. Принципы политики информационной безопасности (УК-2)
57. Основные встроенные механизмы защиты ОС и их недостатки (ОПК-3)
58. Анализ существующих угроз для современных универсальных ОС (ОПК-3)
59. Оценка надежности систем защиты информации (ОПК-3)
60. Задачи и методы резервирования встроенных в ОС механизмов защиты. (ОПК-3)
61. Криптографические методы защиты информации. (ОПК-3)
62. Компьютерные вирусы и механизмы борьбы с ними. (ОПК-3)
63. Профилактика заражения вирусами компьютерных систем. (ОПК-3)
64. Сертификация ИС и ее компонентов по требованиям информационной безопасности. (УК-2)

1.3.2 Оценочные средства для очно-заочной и заочной формам обучения

Практическое занятие №1. Защита интеллектуальной собственности средствами патентного и авторского права; правовая регламентация охранной деятельности.

Контрольные вопросы ПЗ№1 (УК-2, ОПК-3):

1. Если международным договором в области интеллектуальной собственности, в котором участвует РФ, установлены иные правила, чем в законодательстве РФ, то применяются:

2. Система институтов интеллектуальной собственности в настоящее время является подотраслью:

3. Правоотношения в сфере интеллектуальной собственности основаны на принципах:

4. Отличие прав на результаты интеллектуальной деятельности от права собственности заключается в том, что:

5. Объектами интеллектуальной собственности являются:

Практическое занятие №3 Технические средства обеспечения информационной безопасности

1. Поисковое оборудование.

2. Технические средства активного и пассивного противодействия нарушениям информационной безопасности.

Контрольные вопросы ПЗ№3 (УК-2, ОПК-3):

1. Против каких видов утечки информации служит обнаружитель скрытых видеокамер?

2. Для чего нужен панорамный индикатор поля?

3. Для чего нужен панорамный селективный поля?

4. Что такое ПЭМИН?

5. Назовите акустические каналы утечки информации.

6. Назовите каналы электромагнитной утечки информации.

7. С какой целью проводится анализ сигналов?.

8. Какие устройства могут относиться к электронным устройствам негласного получения информации (ЭУНПИ)?

9. Какими функциями обладают анализаторы спектра?

10. С какой целью необходимо подавлять Wi-Fi и другие беспроводные сети связи?

11. Какая информация определяется при проведении радиомониторинга?

12. В какой полосе частот могут функционировать анализаторы радиочастотного спектра?

13. Как может быть осуществлена модуляция голосовой информации (примеры)?

14. Что могут обнаружить системы рентгеновского контроля?

15. Что может обнаруживать нелинейный локатор?

16. В каких случаях применяется нелинейный локатор и в каких – анализатор радиочастотного спектра?

17. Какой принцип противодействия используется в подавителях диктофонов и микрофонов?

18. Какие функции выполняют сетевые фильтры?

19. Какую функцию выполняет акустический сейф?

20. С какой целью на стекла окон устанавливаются вибровозбудители?

21. Какие существуют разновидности генераторов шума?

22. Какой материал используется в экранирующих устройствах?

23. Для чего используются безэховые акустические камеры?

24. Для каких целей используются компьютеры и множительные устройства в защищенно исполнении?

25. Какие параметры измеряются в системах радиомониторинга?

26. Перечислите программные средства, которые могут использоваться для обеспечения информационной безопасности.

Экзаменационные вопросы такие же, как и для студентов очной формы обучения.

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

1.4.1. Порядок и методика проведения промежуточных и итоговой аттестаций

Предусмотрены следующие виды контроля:

- промежуточный контроль по каждому модулю – в форме написания контрольной работы для оценки теоретических знаний;
- промежуточный контроль по каждому модулю – в форме отчетов по лабораторным работам и практическим занятиям для оценки практических навыков;
- итоговый контроль по дисциплине – в форме экзамена.

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 могут быть переведены в оценку:

– «неудовлетворительно» - от 0% до 40% от максимального количества баллов;
– «удовлетворительно» - от 41% до 60% максимального количества баллов;
– «хорошо» - от 61% до 80% максимального количества баллов;
– «отлично» - от 81% до 100% максимального количества баллов.

Для получения зачета студенту достаточно набрать от 41 и более баллов.

Соотношения максимального количества баллов, полученных студентом по блокам модулей, показаны в Таблице 2.

Таблица 2 - Распределение баллов по модулям дисциплины «Основы информационной безопасности сетей и систем»

Модуль	Всего баллов (Максимальное	Теоретический блок (Контрольная работа)	Практический блок (Распределение баллов по
Модуль 1	50	10	40=24+16
Модуль 2	50	10	40=20+20
Модуль - Экзамен	100	100	

Как правило, теоретический блок оценивается по результатам контрольной работы. Практический блок оценивается по результатам выполнения лабораторных работ и заданий на практических занятиях.

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

компетенции данной дисциплины.

1.4.2 Методика проведения экзамена в группах очно-заочной и заочной формам обучения

Экзамен по дисциплине «Основы информационной безопасности сетей и систем» у студентов заочной формы обучения проводится письменно по классической методике. Вопросы сгруппированы в билетах. В каждом билете содержится по 2 теоретических вопроса. Количество билетов должно быть не менее числа студентов в группе. Студенты готовят письменные ответы на вопросы.

2 Методические указания по проведению лабораторных и практических (семинарских) занятий

1. Для подготовки и выполнения практических занятий используются методические разработки: А.Г. Жуковского, размещенные на сайте СКФ МТУСИ в разделе «Методические материалы»: http://www.skf-mtusi.ru/?page_id=659

2. Для подготовки и выполнения лабораторных работ используется учебное пособие: А.Г.Жуковский, Д.А.Жуковский, С.А.Швидченко. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕЙ И СИСТЕМ. – Ростов-на-Дону: СКФ МТУСИ, 2020. – 52 с., размещенная на сайте СКФ МТУСИ в разделе «Методические материалы»: http://www.skf-mtusi.ru/?page_id=659.

3 Образец экзаменационного билета

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

	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 Зав. кафедрой «ИТСС» _____ Юхнов В.И. «____» _____ 20__ г.

Направление подготовки: 11.03.02 ***Инфокоммуникационные технологии и системы связи***
Курсы: 2,3
Дисциплина: ***Основы информационной безопасности сетей и систем***

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. Профессор кафедры «ИТСС» _____ Жуковский А.Г.

4 Вопросы для тестирования (УК-2, ОПК-3)

Данная дисциплина формирует у выпускника 2-х компетенции, которые связаны, взаимодействуют между собой и объективно оценить каждую в отдельности при ответе студента на контрольный вопрос тестового задания по проверке уровня остаточных знаний достаточно сложно. Предлагается считать, что вклад 2-х компетенций в общую оценку при ответе на вопрос примерно одинаков.

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

1) К правовым методам, обеспечивающим информационную безопасность, относятся:
- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
- Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:
- Хищение жестких дисков, подключение к сети, инсайдерство
- Перехват данных, хищение данных, изменение архитектуры системы
- Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:
- Персональная, корпоративная, государственная
- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:
- несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций

5) Основные объекты информационной безопасности:
- Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:
- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
- Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:
- Экономической эффективности системы безопасности
- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:
- руководители, менеджеры, администраторы компаний
- органы права, государства, бизнеса
- сетевые базы данных, файерволы

9) К основным функциям системы безопасности можно отнести все перечисленное:
- Установление регламента, аудит системы, выявление рисков
- Установка новых офисных приложений, смена хостинг-компании
- Внедрение аутентификации, проверки контактных данных пользователей

10) Принципом информационной безопасности является принцип недопущения:
- Неоправданных ограничений при работе в сети (системе)
- Рисков безопасности сети, системы
- Презумпции секретности

11) Принципом политики информационной безопасности является принцип:
- Невозможности миновать защитные средства сети (системы)
- Усиления основного звена сети, системы
- Полного блокирования доступа при риск-ситуациях

12) Принципом политики информационной безопасности является принцип:
- Усиления защищенности самого незащищенного звена сети (системы)
- Перехода в безопасное состояние работы сети, системы
- Полного доступа пользователей ко всем ресурсам сети, системы

13) Принципом политики информационной безопасности является принцип:
- Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- Одноуровневой защиты сети, системы
- Совместимых, однотипных программно-технических средств сети, системы

14) К основным типам средств воздействия на компьютерную сеть относится:
- Компьютерный сбой
- Логические закладки («мины»)
- Аварийное отключение питания

15) Когда получен спам по e-mail с приложенным файлом, следует:
- Прочитать приложение, если оно не содержит ничего ценного – удалить
- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
- Удалить письмо с приложением, не раскрывая (не читая) его

16) Принцип Кирхгофа:
- Секретность ключа определена секретностью открытого сообщения
- Секретность информации определена скоростью передачи данных
- Секретность закрытого сообщения определяется секретностью ключа

17) ЭЦП – это:
- Электронно-цифровой преобразователь
- Электронно-цифровая подпись
- Электронно-цифровой процессор

18) Наиболее распространены угрозы информационной безопасности корпоративной системы:
- Покупка нелицензионного ПО
- Ошибки эксплуатации и неумышленного изменения режима работы системы
- Сознательного внедрения сетевых вирусов

19) Наиболее распространены угрозы информационной безопасности сети:

- Распределенный доступ клиент, отказ оборудования
- Моральный износ сети, инсайдерство
- Сбой (отказ) оборудования, нелегальное копирование данных

20) Наиболее распространены средства воздействия на сеть офиса:
- Слабый трафик, информационный обман, вирусы в интернет
- Вирусы в сети, логические мины (закладки), информационный перехват
- Компьютерные сбои, изменение администрирования, топологии

21) Утечкой информации в системе называется ситуация, характеризуемая:
- Потерей данных в системе
- Изменением формы информации
- Изменением содержания информации

22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
- Целостность
- Доступность
- Актуальностьl

23) Угроза информационной системе (компьютерной сети) – это:
- Вероятное событие
- Детерминированное (всегда определенное) событие
- Событие, происходящее периодически

24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
- Регламентированной
- Правовой
- Защищаемой

25) Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:
- Программные, технические, организационные, технологические
- Серверные, клиентские, спутниковые, наземные
- Личные, корпоративные, социальные, национальные

26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:
- Владелец сети
- Администратор сети
- Пользователь сети

27) Политика безопасности в системе (сети) – это комплекс:
- Руководств, требований обеспечения необходимого уровня безопасности
- Инструкций, алгоритмов поведения пользователя в сети
- Нормы информационного права, соблюдаемые в сети

28) Наиболее важным при реализации защитных мер политики безопасности является:
- Аудит, анализ затрат на проведение защитных мер
- Аудит, анализ безопасности
- Аудит, анализ уязвимостей, риск-ситуаций

29) Очень сложные пароли гарантируют 100% защиту?
А.Нет
Б.Да, если после работы полностью очищать куки и не хранить пароль на компьютере
В.Да, если пароль не сохранен на компьютере

30.Какие вирусы активизируются после включения ОС?
А.Сниффферы
Б.Загрузочные
В.Трояны
Г.Черви

31.Представляют ли угрозу вирусы для крупных компаний?
А.Нет
Б.Да, представляют
В.Скорее нет. В крупных компаниях развита система безопасности
Г.Если компания обладает сотрудниками занимающимися безопасностью сети, вирусы не могут нанести такому предприятию вреда

32.С чем связана атака введением произвольных запросов в базу данных?
А.Уязвимость SQL Injection
Б.Сбой Denial of Service
В.Ошибка Denial of Service
Г.Неполадка PHP Include

33.Фильтрация контента, для чего она служит?
А.Защищает от скрытой загрузки вредоносного программного обеспечения +
Б.Помогает быстро находить в сети требуемый контент сохраняя при этом много драгоценного времени
В.Отключает назойливую рекламу
Г.Отсеивает поисковый спам

34.Какой уровень безопасности трафика обеспечивает WPA2?
А.Высокий
Б.Низкий
В.Достаточный для домашней сети
Г.Средний

35.Сколько минимально символов должен содержать безопасный пароль, состоящий из латинских строчных букв?
А.15
Б.8
В.10
Г.6

36.Какую угрозу можно назвать преднамеренной? Сотрудник:
А.Открыл письмо содержащее вредоносное ПО
Б.Ввел неправильные данные
В.Совершил не авторизованный доступ
Г.Включил компьютер без разрешения

37. Безопасно ли вводить пароли простым копированием?
А.Безопасно если это мой компьютер

Б.Да
В.Безопасно если после работы очистить куки
Г.Нет

38.Какую защиту необходимо использовать против программы iris или ее аналогов?
А.Шифровать трафик
Б.Использовать очень сложные пароли
В.Устанавливать только лицензионные антивирусы
Г.Не пользоваться Wi-fi

39. Что может привести к заражению компьютера?
А.Получение сообщения по электронной почте
Б.Загрузка пиратского ПО
В.Создание нового файла
Г.Отправка сообщения по электронной почте

40. Что такое Brute Force?
А.Взлом методом заражения системы через вредоносный файл
Б.Метод заставляющий пользователя самому раскрыть конфиденциальную информацию
В.Получение конфиденциальной информации с компьютера методом электронной рассылки
Г.Взлом методом перебора паролей

41. В каком блок файле autorun.inf чаще всего прописывается вредоносная программа?
А.Open
Б.Setup
В.Downloade
Г.Dll

42. Как называется преднамеренно внесенный в программное обеспечение объект, приводящий к действиям программного обеспечения не предусмотренным производителем, приводящим к нарушению конфиденциальности и целостности информации?
А.Троян
Б.Бэкдор
В.Закладка
Г.Вирус

43. Безопасно ли сохранять пароли в автозаполнении браузера?
А.Да, если пароль к входу в систему знаю только я один
Б.Нет
В.Да, если этим компьютером пользуюсь только я один
Г.Да

44. Для чего служит DLP? Система выполняет функцию:
А.Защита компьютера от вирусов
Б.Выполняет функцию безопасного ввода паролей
В.Предотвращает утечку информации с компьютера
Г.Предупреждает пользователя о попытках взлома и хакерских атаках

45. Антивирус полностью защищает компьютер от вирусов и атак при работе в сети. Вы согласны с этим?
А.Нет
Б.Да, если это лицензионный антивирус известного производителя

В.Защищает совместно с включенным бродмауэром
Г.Да

46. Самый лучший способ хранения паролей в информационной системе?
А.Хеширование
Б.Вообще не сохранять
В.Архивирование
Г.Хранить только с включенным брандмауэром

47. Какое минимальное количество символов должен содержать пароль входа субъектов в систему АС, при классе защищенности 1А?
А.12
Б.8
В.10
Г.15

48. На каких системах более динамично распространяются вирусы?
AL.inux
Б.MacOS
В.Android
Г.Windows

49. Самая массовая угроза компьютерной безопасности, это:
А.Спам
Б.Трояны
В.Черви
Г.Шпионские программы

50. Если компьютер работает в нормальном режиме, означает ли это что он не заражен?
А.Нет
Б.Если не изменилась скорость работы, компьютер совершенно чист
В.Да
Г.Если антивирус ничего не показывает компьютер чист

51. Установка одновременно нескольких антивирусных программ повышает защищенность. Вы согласны с этим?
А.Да
Б.Да, если это антивирусы от известных производителей
В.Да, если это антивирусы одного производителя
Г.Нет

52. Что чаше всего используют злоумышленники при атаке на компьютеры должностных лиц и руководителей крупных компаний?
А.Фишинг
Б.Спам
В.Загрузка скрытого вредоносного ПО
Г.DDos атаки

53. Как гарантировать 100% защищенность компьютера от заражения вирусами в сети?
А.Включить брандмауэр
Б.Установить новое программное обеспечение
В.Таких гарантий нет

Г.Посещать только сайты известных брендов

54. Что необходимо выполнять для контроля безопасности электронной почты?
А.Часто сменять пароли
Б.Проверять страницу посещения
В.Регистрировать почтовый ящик только в известных системах
Г.Использовать сложные пароли

55. Что такое Firewall, для чего он нужен?
А.для фильтрации трафика
Б.для очистки компьютера
В.для быстрого и безопасного поиска информации
Г.для форматирования

56. Обеспечивает ли форматирование жесткого диска полное избавление от вирусов?
А.Обеспечивает полностью
Б.Обеспечивает если выполнено быстрое форматирование
В.Нет
Г.Обеспечивает при низкоуровневом форматировании

57. Можно ли хранить важную информацию на жестком диске компьютера, в том числе пароли?
А.Да, если это мой личный компьютер
Б.Да
В.Нет
Г.Да, если компьютер не подключен к интернету

58. Если, не нажимая на иконки просто просмотреть подозрительный сайт, ничего не произойдет. Вы согласны?
А.Нет. Заражение может произойти, даже если вы просто посмотрели информацию с экрана, при этом ничего не нажимая
Б.Да, простой просмотр не наносит никакого вреда
В.Да, заражение происходит только после кликов, чем запускается вирусная программа.

59. Что такое государственная тайна?
1) Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ
2) Сведения о состоянии окружающей среды
3) Все сведения, которые хранятся в государственных базах данных
4) Сведения о состоянии здоровья президента РФ
5) Конкретные сведения, в отношении которых компетентные органы и их должностные лица приняли решение об их отнесении к государственной тайне

60. Что такое коммерческая тайна?
1) Информация, имеющая действительную или потенциальную коммерческую ценность в силу ее неизвестности третьим лицам
2) Информация, к которой нет доступа на законном основании
3) Информации, обладатель которой принимает меры к охране ее конфиденциальности
4) Информация, содержащая в учредительных документах
5) Информация, содержащая в годовых отчетах, бухгалтерских балансах, формах государственных статистических отчетов

8.2 Методика оценивания остаточных знаний

Максимальное время выполнения теста - 60 минут.

Количество вопросов в тестовом задании - 60.

Для проведения контроля остаточных знаний компьютер формирует в случайном порядке тестовые вопросы.

При прохождении тестового контроля знаний студент должен выбрать один или несколько правильных ответов на один из вопросов тестового задания.

В случае правильного ответа на 49 и более тестовых вопросов (>81%) студент подтверждает освоение компетенций с оценкой «отлично», при ответе на 48-37 вопросов (61-80%) студент подтверждает освоение компетенций с оценкой «хорошо», при ответе н на 36-25 вопросов (41-60%) студент подтверждает освоение компетенций с оценкой «удовлетворительно», при ответе менее чем на 25 вопросов (<41%) студент не подтверждает необходимый уровень знаний и оценивается неудовлетворительно.

Дополнения и изменения в ОМ