Министерство науки и высшего образования РФ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.07 ОСНОВЫ ЦИФРОВОЙ БЕЗОПАСНОСТИ В СЕРВИСНОЙ ДЕЯТЕЛЬНОСТИ

Направление подготовки (специальность) 43.04.01 Сервис

Профиль подготовки (специализация) 43.04.01.02 Цифровые технологии в сервисной деятельности

Форма обучения очная

Год набора 2024

Красноярск 2025

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Программу составили
доцент,канд. техн. наук Нечушкина Елена Алексеевна

1 Цели и задачи изучения дисциплины

1.1 Цель преподавания дисциплины:

расширение и конкретизация знаний об основах цифровой безопасности на предприятиях сферы сервиса, усвоение конкретных правил и приёмов защиты информации.

1.2 Задачи изучения дисциплины:

- формирование знаний об информации в развитии современного цифрового общества;

− формирование умений анализировать средства цифровой безопасности;

- формирование навыков применения современных технических средств при защите информации.

1.3 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы высшего образования:

Код и наименование индикатора достижения компетенции	Запланированные результаты обучения по дисциплине
ПК-2 Способен применять научные концепции исследования и моделирования для обоснования стратегических решений по развитию предприятий в сервисной деятельности	
ПК-2.1 Производит выбор научных концепций и методов исследования и моделирования сервисной деятельности	- Выбирает научные концепции для идентификации текущих и возможных угроз цифровой безопасности; - Осуществляет выбор методов исследования и моделирования угроз цифровой безопасности и управления ими
ПК-2.2 Обосновывает стратегические решения по развитию сервисной деятельности предприятия на основе научных концепций и современных методов исследования и моделирования	- Описывает стратегические решения по развитию предприятий в сервисной деятельности с учетом интеграции цифровых решений в систему управления; - Осуществляет моделирование событий, сценариев и алгоритмов действий с использованием современных методов исследования цифровой безопасности; - Применяет современные методы исследования для обеспечения уровня сервиса в области защиты киберсреды предприятия и пользователей

Дисциплина реализуется без применения ЭО и ДОТ

2 Объем дисциплины (модуля)

Вид учебной работы	Всего, зачетных единиц (акад.час)	Семестр
		1
Общая трудоемкость дисциплины	2 (72)	2 (72)
Контактная работа с преподавателем:	0,7 (24)	0,7 (24)
занятия лекционного типа	0,3 (12)	0,3 (12)
лабораторные работы	0,3 (12)	0,3 (12)
Самостоятельная работа обучающихся	1,3 (48)	1,3 (48)
Вид промежуточной аттестации (Зачет)		Зачёт

3 Содержание дисциплины (модуля)

№ п/п	Вид работ	Темы занятия	Объем часов	Семестр /курс	Часы в эл. формате
Раздел 1. Цифровая безопасность: характеристика, элементы, функции классификация					
1.	Лек	Цифровая безопасность: характеристика, элементы, функции классификация	3	1	
2.	Лаб	Цифровая безопасность: научные концепции исследования	2	1	
3.	Ср	Цифровая безопасность: научные концепции моделирования стратегии	12	1	
Раздел 2. Методические аспекты оценки рисков цифровой безопасности с учетом отраслевой специфики					
1.	Лек	Методические аспекты оценки рисков цифровой безопасности с учетом отраслевой специфики	3	1	
2.	Лаб	Методические аспекты оценки рисков цифровой безопасности с учетом отраслевой специфики	2	1	
3.	Ср	Методические аспекты оценки рисков цифровой безопасности с учетом отраслевой специфики	12	1	
Раздел 3. Методы экономической оценки рисков цифровой безопасности					
1.	Лек	Методы экономической оценки рисков цифровой безопасности	3	1	
2.	Лаб	Методы экономической оценки рисков цифровой безопасности	4	1	
3.	Ср	Методы экономической оценки рисков цифровой безопасности	12	1	
Раздел 4. Пути снижения цифровых рисков в современных условиях					
1.	Лек	Пути снижения цифровых рисков в современных условиях	3	1	
2.	Лаб	Разработка стратегических решений по развитию цифровой безопасности предприятий	4	1	
3.	Ср	Пути снижения цифровых рисков в современных условиях	12	1	
4.	Зачёт			1	

4 Учебно-методическое обеспечение дисциплины

4.1 Печатные и электронные издания:

1. Глинская Е. В., Чичварин Н. В. Информационная безопасность конструкций ЭВМ и систем:Учебное пособие. - Москва: ООО "Научно-издательский центр ИНФРА -М", 2018. - 118 с..

2. Белько Е. С., Богульская Н. А. Информационная безопасность [Электронный ресурс]:учебно-методическое пособие. - Красноярск: СФУ, 2018. - – Режим доступа: http://Lib3.sfu-kras.ru/ft/LIB2/ELIB/u004/i-634391942.pdf .

3. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации:Учебное пособие. - Москва: Издательский Центр РИО□, 2018. - 336 с..

4. Баранова Е.К., Бабаш А.В. Информационная безопасность. История специальных методов криптографической деятельности [Электронный ресурс]:Учебное пособие. - Москва: Издательский Центр РИО□, 2019. - 236 с. – Режим доступа: https://znanium.com/catalog/document?id=326176 .

5. Гришина Н. В. Информационная безопасность предприятия [Электронный ресурс]:Учебное пособие. - Москва: Издательство "ФОРУМ", 2019. - 239 с. – Режим доступа: https://znanium.com/catalog/document?id=362851 .

6. Партыка Т. Л., Попов И. И. Информационная безопасность [Электронный ресурс]:Учебное пособие. - Москва: Издательство "ФОРУМ", 2019. - 432 с. – Режим доступа: https://znanium.com/catalog/document?id=327912 .

7. Мытник К. Я., Панасенко С. П. Смарт-карты и информационная безопасность [Электронный ресурс]:научное издание. - Москва: ДМК Пресс, 2018. - 516 с. – Режим доступа: https://e.lanbook.com/book/116128 .

8. Басыня Е. А. Системное администрирование и информационная безопасность [Электронный ресурс]:учеб. пособие. - Новосибирск: НГТУ, 2018. - 79 с. – Режим доступа: https://e.lanbook.com/book/118259 .

9. Минзов А. С., Бобылева С. В., Осипов П. А., Попов А. А. Информационная безопасность и защита информации [Электронный ресурс]:практикум. - Дубна: Государственный университет «Дубна», 2020. - 85 с. – Режим доступа: https://e.lanbook.com/book/154490 .

10. Информационная безопасность: современная теория и практика: сборник научных трудов студентов, аспирантов и преподавателей по материалам II Межвузовской научно-практической конференции [Электронный ресурс]:. - Омск: СибАДИ, 2019. - 145 с. – Режим доступа: https://e.lanbook.com/book/163756 .

4.2 Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства (программное обеспечение, на которое университет имеет лицензию, а также свободно распространяемое программное обеспечение):

1. Microsoft Office Professional Plus 2007 Russian Academic. Офисный пакет Microsoft Office.

4.3 Интернет-ресурсы, включая профессиональные базы данных и информационные справочные системы:

1. Электронная правовая система "КонсультантПлюс". https://www.consultant.ru

Электронная правовая система "КонсультантПлюс"

Электронно- правовая ситтема «Система ГАРАНТ»

2. Электронно- правовая ситтема «Система ГАРАНТ». https://ivo.garant.ru

Электронная правовая система "КонсультантПлюс"

Электронно- правовая ситтема «Система ГАРАНТ»

3. Официальный сайт Федеральной службы государственной статистики http://www.gks.ru

4. Официальный сайт Центрального Банка РФ http://www.cbr.ru

5. Официальный сайт Министерства экономического развития РФ http://www.economy.gov.ru

6. Поисковая система Google https://www.google.ru/
7. Поисковая система Яндекс https://www.yandex.ru/
8. Поисковая система Mail https://www.mail.ru/
9. Министерство финансов РФ http://www.minfin.ru/
10. ИАС «Статистика» http://www.ias-stat.ru/

5 Фонд оценочных средств

Фонд оценочных средств является приложением к рабочей программе дисциплины (модуля), хранится на кафедре, обеспечивающей преподавание данной дисциплины (модуля).

6 Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю)

Кафедра располагает материально-технической базой, обеспечивающей проведение всех видов дисциплинарной и междисциплинарной подготовки, практической и научно-исследовательской работы студентов, предусмотренных учебным планом подготовки и соответствующей действующим санитарным и противопожарным правилам и нормам.

В учебном процессе по дисциплине для проведения учебных занятий лекционного типа, семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются учебные аудитории в соответствии с расписанием занятий.

Учебные аудитории укомплектованы специализированной мебелью, демонстрационным оборудованием и техническими средствами обучения (экран, проектор, доска учебная, ноутбук, АРМ студента).

Помещения для самостоятельной работы студентов оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и доступа в электронную информационно-образовательную среду университета (ЭИОС).

Освоение дисциплины инвалидами и лицами с ограниченными возможностями здоровья осуществляется с использованием средств обучения общего назначения.

учебная аудитория для проведения лекционных, семинарских и практических занятий: Специализированная мебель, демонстрационное оборудование, АРМ преподавателя, подключение к сети «Интернет» и индивидуальный неограниченный доступ в ЭИОС университета

Компьютерный класс: Компьютеры, проектор

учебная аудитория для проведения практических занятий: Специализированная мебель, демонстрационное оборудование, специальное оборудование в соответствии со спецификой дисциплины, подключение к сети «Интернет» и индивидуальный неограниченный доступ в ЭИОС университета

Министерство науки и высшего образования РФ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине	Б1.В.07 Основы цифровой безопасности в сервисной деятельности
Направление подготовки / специальность	43.04.01 «Сервис»
Направленность (профиль)	43.04.01.02 Цифровые технологии в сервисной деятельности

Красноярск 2025

1 Перечень компетенций с указанием индикаторов их достижения, соотнесенных с результатами обучения по дисциплине (модулю), практики и оценочными средствами

Семестр	Код и содержание индикатора компетенции	Результаты обучения	Оценочные средства по каждому индикатору достижения компетенции
ПК-2: Способен применять научные концепции исследования и моделирования для обоснования стратегических решений по развитию предприятий в сервисной деятельности			
1	ПК-2.1. Производит выбор научных концепций и методов исследования и моделирования сервисной деятельности	Выбирает научные концепции для идентификации текущих и возможных угроз цифровой безопасности	Тестовые задания, тематика рефератов, вопросы к зачету
		Осуществляет выбор методов исследования и моделирования угроз цифровой безопасности и управления ими	Тестовые задания, тематика рефератов, вопросы к зачету
	ПК-2.2. Обосновывает стратегические решения по развитию сервисной деятельности предприятия на основе научных концепций и современных методов исследования и моделирования	Описывает стратегические решения по развитию предприятий в сервисной деятельности с учетом интеграции цифровых решений в систему управления	Тестовые задания, тематика рефератов, вопросы к зачету
		Осуществляет моделирование событий, сценариев и алгоритмов действий с использованием современных методов исследования цифровой безопасности	Тестовые задания, тематика рефератов, вопросы к зачету
		Применяет современные методы исследования для обеспечения уровня сервиса в области защиты киберсреды предприятия и пользователей	Тестовые задания, тематика рефератов, вопросы к зачету

2 Типовые оценочные средства или иные материалы, с описанием шкал оценивания и методическими материалами, определяющими процедуру проведения и оценивания достижения результатов обучения

Реферат

Тематика рефератов

1. Классификация информации. Виды данных и носителей.
2. Ценность информации. Цена информации.
3. Количество и качество информации.
4. Виды защищаемой информации.
5. Демаскирующие признаки объектов защиты.
6. Классификация источников и носителей информации.
7. мероприятия по управлению доступом к информации.
8. Функциональные источники сигналов. Опасный сигнал.
9. Основные средства и системы, содержащие потенциальные источники опасных сигналов.
10. Вспомогательные средства и системы, содержащие потенциальные источники

опасных сигналов.

11. Виды паразитных связей и наводок, характерные для любых радиоэлектронных средств и проводов, соединяющих их кабелей.

12. Виды угроз безопасности информации.

13. Основные принципы добывания информации.

14. Процедура идентификации, как основа процесса обнаружения объекта.

15. Методы синтеза информации.

16. Методы несанкционированного доступа к информации.

17. Основными способами привлечения сотрудников государственных и коммерческих структур, имеющих доступ к интересующей информации.

18. Способы наблюдения с использованием технических средств.

19. Каналы утечки информации. Технические каналы утечки

20. Классификация технических каналов утечки по физической природе носителя.

21. Классификация технических каналов утечки по информативности.

22. Классификация технических каналов утечки по времени функционирования.

23. Классификация технических каналов утечки по структуре.

24. Наблюдение в оптическом диапазоне и применяемые для этого средства. Характеристики таких средств.

25. Перехват электромагнитных излучений.

26. Акустическое подслушивание. Эффекты, возникающие при подслушивании.

27. Понятия скрытия информации, виды скрытий. Информационный портрет.

28. Противодействие наблюдению. Способы маскировки.

29. Способы и средства противодействия подслушиванию.

30. Нейтрализация закладных устройств.

31. Состав инженерной защиты и технической охраны объектов.

32. Инженерные конструкции и сооружения для защиты информации. Их классификация.

33. Средства идентификации личности.

Классификация датчиков охранной сигнализации.

35. Классификация извещателей.

36. Телевизионные системы наблюдения.

37. Основные средства системы видеоконтроля.

38. Защита личности как носителя информации.

39. Системный подход к защите информации.

40. Параметры системы защиты информации.

41. этапы проектирования системы защиты информации.

42. Потенциальные каналы утечки информации.

Этапы разработки мер по предотвращению угроз утечки информации.

44. Угрозы сохранности данных в компьютере случайного характера.

45. Устройства электропитания компьютера, применяемые для защиты компьютера от неблагоприятных воздействий питающей электросети.

46. Дефекты магнитных дисков.

47. Простые приемы, используемые для защиты компьютера от умышленных действий.

48. Классификация вирусов.

49. Классификация антивирусных программ.

50. Компьютерная преступность. Виды преступной деятельности.

51. Преступления, связанные с нарушением частной тайны.

52. Информационные процессы.

53. Информационные технологии и их основные свойства.

Понятия сигнала, сообщения и данных.

55. Методы защиты информации от преднамеренного доступа.

56. Методы обеспечения безопасности каналов передачи данных.

57. Методы обеспечения достоверности передачи информации (методов защиты от ошибок).

58. Механизмы обеспечения безопасности радиолиний.

59. Криптографическая защита информации (основные понятия).

60. Методы шифрования данных.

61. Стандарт шифрования данных DES.

Методические указания по выполнению рефератов

Реферат представляет собой сокращенный пересказ содержания первичного документа (или его части) с основными фактическими сведениями и выводами. Написание реферата используется в учебном процессе вуза в целях приобретения студентом необходимой профессиональной подготовки, развития умения и навыков самостоятельного научного поиска: изучения литературы по выбранной теме, анализа различных источников и точек зрения, обобщения материала, выделения главного, формулирования выводов и т. п. С помощью рефератов студент глубже постигает наиболее сложные проблемы курса, учится лаконично излагать свои мысли, правильно оформлять работу, докладывать результаты своего труда.

Процесс написания реферата включает:

- выбор темы;
- подбор нормативных актов, специальной литературы и иных источников, их изучение;
- составление плана;
- написание текста работы и ее оформление;
- устное изложение реферата.

Рефераты пишутся по наиболее актуальным темам. В них на основе тщательного анализа и обобщения научного материала сопоставляются различные взгляды авторов и определяется собственная позиция студента с изложением соответствующих аргументов.

Темы рефератов должны охватывать и дискуссионные вопросы курса. Они призваны отражать передовые научные идеи, обобщать тенденции практической деятельности, учитывая при этом изменения в текущем законодательстве.

Рекомендованная выше тематика рефератов примерная. Студент при желании может сам предложить ту или иную тему, предварительно согласовав ее с преподавателем.

Реферат состоит из введения, в котором кратко обосновывается актуальность, научная и практическая значимость избранной темы, основного материала, содержащего суть проблемы и пути ее решения, и заключения, где формируются выводы, оценки, предложения.

Объем реферата - от 5 до 15 машинописных страниц. Содержание реферата студент докладывает на семинаре, научной конференции. Предварительно подготовив тезисы доклада, студент в течение 5-7 минут должен кратко изложить основные положения своей работы. После доклада автор отвечает на вопросы, затем выступают оппоненты, которые заранее познакомились с текстом реферата, и отмечают его сильные и слабые стороны. На основе обсуждения студенту выставляется соответствующая оценка.

Критерии оценки:

Оценка «зачтено» ставится, если реферат соответствует всем требованиям к письменным работам данного уровня. Могут быть незначительные замечания по содержанию и оформлению работы. Доклад изложен грамотным языком, свидетельствующим об овладении специальной терминологией и свободном понимании и владении понятиями. На возникшие у преподавателя дополнительные вопросы студент должен давать четкие и конкретные ответы, показывая умение выделять существенные и несущественные моменты материала.

Оценка «незачтено» ставится, если есть существенные замечания к оформлению и содержанию письменной работы. Кроме того, при изложении материала студент не владеет им свободно, на теоретические вопросы даны неправильные ответы, свидетельствующие о том, что студент не усвоил понятия, у него не сформирован комплекс основных знаний по теме, в ответах отсутствует логика изложения, выводы, обобщения.

Тестовые задания закрытого и открытого типа по дисциплине

Прочитайте текст, выберите все правильные варианты

1. К правовым методам, обеспечивающим информационную безопасность, относятся:

1. Разработка аппаратных средств обеспечения правовых данных
2. Разработка и установка во всех компьютерных правовых сетях журналов учета действий
3. Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2. Основными источниками угроз цифровой безопасности являются все указанное в списке:

1. Хищение жестких дисков, подключение к сети, инсайдерство
2. Перехват данных, хищение данных, изменение архитектуры системы
3. Хищение данных, подкуп системных администраторов, нарушение регламента работы

3. Виды информационной безопасности:

1. Персональная, корпоративная, государственная
2. Клиентская, серверная, сетевая
3. Локальная, глобальная, смешанная

4. Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:

1. Регламентированной
2. Правовой
3. Защищаемой

5. Разновидностями угроз безопасности (сети, системы) являются все перечисленное в списке:

1. Программные, технические, организационные, технологические
2. Серверные, клиентские, спутниковые, наземные
3. Личные, корпоративные, социальные, национальные

Дополните предложение

6. Цели цифровой безопасности – своевременное обнаружение, предупреждение_____.

Прочитайте текст и установите соответствие.

7. К каждой позиции, данной в левом столбце, подберите соответствующую позицию из правого столбца:

Понятие	Сущность
1 Основные объекты информационной безопасности	А органы права, государства, бизнеса
2 Основные риски цифровой безопасности	Б экономическая эффективность системы безопасности
3 Основные принципы обеспечения цифровой безопасности	В потеря, искажение, утечка информации
4 Основные субъекты цифровой безопасности	Г установление регламента, аудит системы, выявление рисков
5 Основным функции системы безопасности	Д компьютерные сети, базы данных

8. К каждой позиции, данной в левом столбце, подберите соответствующую позицию из правого столбца:

Принцип политики цифровой безопасности	Сущность
1 Недопущения	А обхода защитных средств сети (системы)
2 Невозможности	Б защищенности самого незащищенного звена сети (системы)
3 Усиления	В доступа (обязанностей, привилегий) клиентам сети (системы)
4 Разделения	Г неоправданных ограничений при работе в сети (системе)

9. Установите соответствие:

Наиболее распространены	Сущность
1 угрозы цифровой безопасности сети	А Ошибки эксплуатации и неумышленного изменения режима работы системы
2 угрозы цифровой безопасности корпоративной системы	Б Сбой (отказ) оборудования, нелегальное копирование данных
3 средства воздействия на сеть офиса	В Вирусы в сети, логические мины (закладки), информационный перехват

Дополните определение

10. Логические закладки («мины») относятся к _____ на компьютерную сеть.

11. Когда получен спам по e-mail с приложенным файлом, следует_____.

12. Выражение «секретность закрытого сообщения определяется секретностью ключа» - отражает _____.

13. _____ занимается обеспечением скрытности информации в информационных массивах.

14. _____ называется запись определенных событий в журнал безопасности сервера.

15. _____ называется конечное множество используемых для кодирования информации знаков.

16. _____ называется конфигурация из нескольких компьютеров, выполняющих общее приложение.

17. _____ называется метод управления доступом, при котором каждому объекту системы присваивается метка критичности, определяющая ценность информации.

18. _____ называется нормативный документ, регламентирующий все аспекты безопасности продукта информационных технологий.

19. _____ называется оконечное устройство канала связи, через которое процесс может передавать или получать данные.

20. _____ обеспечивается защита исполняемых файлов.

21. _____ обеспечивается защита от программных закладок.

22. _____ обеспечивается защита от форматирования жесткого диска со стороны пользователей.

23. _____ объединяет математические методы нарушения конфиденциальности и аутентичности информации без знания ключей.

24. _____ определяется как предотвращение возможности отказа одним из участников коммуникаций от факта участия в передаче данных.

25. _____ создается для реализации технологии RAID.

26. _____ составляет основу политики безопасности.

27. _____ управляет регистрацией в системе Windows 2000.

28. _____ уровень ОС определяет взаимодействие с глобальными ресурсами других организаций.

29. _____ уровень ОС связан с доступом к информационным ресурсам внутри организации.

30. _____ характеризует соответствие средств безопасности решаемым задачам.

31. _____ является администратором базы данных.

32. _____ является достоинством дискретных моделей политики безопасности.

33. "Троянский конь" является разновидностью модели воздействия программных закладок_____

34. "Уполномоченные серверы" были созданы для решения проблемы_____

35. "Уполномоченные серверы" фильтруют пакеты на уровне_____

36. ACL-список ассоциируется с каждым_____

37. Абстрактное описание системы, без связи с ее реализацией, дает модель политики безопасности

38. Административные действия в СУБД позволяют выполнять привилегии

39. Администратор _____ занимается регистрацией пользователей СУБД.

40. Администратор сервера баз данных имеет имя_____

41. Битовые протоколы передачи данных реализуются на _____ уровне модели взаимодействия открытых систем.

Методические рекомендации по выполнению:

Тестовые задания рассчитаны на самостоятельную работу безиспользования вспомогательных материалов. То есть при их выполнении не следует пользоваться текстами законов, учебниками, литературой и т.д. Основные задачи выполнения тестовых заданий:

1) закрепление полученных ранее теоретических знаний;

2) выработка навыков самостоятельной работы;

3) выяснение подготовленности студента к будущей практической работе.

Для выполнения тестового задания, прежде всего, следует внимательно прочитать поставленный вопрос. После ознакомления с вопросом следует приступать к прочтению предлагаемых вариантов ответа. Необходимо прочитать все варианты и в качестве ответа следует выбрать лишь один индекс (цифровое обозначение), соответствующий правильному ответу. Тесты составлены таким образом, что в каждом из них правильным является лишь один из вариантов. Выбор должен быть сделан в пользу наиболее полного ответа.

На выполнение теста отводится ограниченное время. Время выполнения тестового задания определяется из расчета 30-45 секунд на один вопрос.

Критерии оценивания:

Оценка (стандартная)	Оценка (тестовые нормы: % правильных ответов)
«отлично»	80-100 %
«хорошо»	70-79%
«удовлетворительно»	60-69%
«неудовлетворительно»	менее 60%

Перечень вопросов для промежуточной аттестации (зачет)

Цель зачета – проверка уровня усвоения студентами учебного материала, предусмотренного программой, и способности адаптировать полученные знания к

профессиональной деятельности в современных условиях. Зачет по дисциплине проводится в следующих формах:
- устное собеседование по программным вопросам курса;
- письменный ответ студента на поставленные вопросы.

Вопросы к зачету

1. Защита информации. Общие представления
2. Информационно-манипулятивные технологии (социальная инженерия)
3. Информационная система как объект защиты
4. Объекты и предметы защиты
5. Виды защищаемой информации
6. Угрозы безопасности информации и их классификация.
7. Основные угрозы конфиденциальности
8. Основные угрозы целостности
9. Основные угрозы доступности
10. Основные источники внутренних угроз в информационной системе организации сферы услуг
11. Классификация нарушителей
12. Модель нарушителя
13. Идентификация и аутентификация. Метод пароля и его модификация.
14. Идентификация и аутентификация Защита информации с помощью идентификационных карт
15. Идентификация и аутентификация. Биометрические системы защиты. Основные представления
16. Алгоритм использования биометрического признака при идентификации и аутентификации личности. Ошибки первого и второго рода
17. Стеганография как способ защиты информации
18. Проверка целостности файлов: основные представления
19. Способы восстановлены удаленных данных
20. Способы безвозвратного удаления данных
21. Механизмы защиты информации: основные представления
22. Использование полиграфа для решения задач защиты информации: общие представления
23. Средства защиты информации: общие представления
24. Графический пароль: общие представления
25. Подсистемы информационной безопасности
26. Защита информации: меры
27. Защита информации: методы
28. Защита информации: этапы реализации механизмов защиты
29. Защита информации: уровни безопасности
30. Характеристика основных цифровых подписей

Методические рекомендации по подготовке к промежуточной аттестации (зачет)

Готовиться к зачету необходимо последовательно, с учетом контрольных вопросов, разработанных преподавателем. Сначала следует определить место каждого контрольного вопроса в соответствующем разделе темы учебной программы, а затем внимательно прочитать и осмыслить рекомендованные научные работы, соответствующие разделы рекомендованных учебников. При этом полезно делать хотя бы самые краткие выписки и заметки. Работу над темой можно считать завершенной, если вы сможете ответить на все контрольные вопросы и дать определение понятий по изучаемой теме.

Для обеспечения полноты ответа на контрольные вопросы и лучшего запоминания теоретического материала рекомендуется составлять план ответа на контрольный вопрос. Это позволит сэкономить время для подготовки непосредственно перед зачетом за счет обращения не к литературе, а к своим записям.

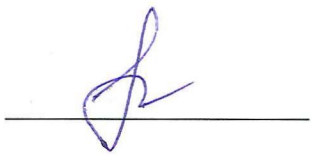
При подготовке необходимо выявлять наиболее сложные, дискуссионные вопросы, с тем, чтобы обсудить их с преподавателем на обзорных лекциях и консультациях.

Нельзя ограничивать подготовку к экзамену простым повторением изученного материала. Необходимо углубить и расширить ранее приобретенные знания за счет новых идей и положений.

Критерии оценки:

Оценка «зачтено» ставится, если дан полный и развернутый ответ на поставленные вопросы и правильно, без ошибок и погрешностей. Ответы на вопросы должны свидетельствовать о совокупности осознанных знаний об объекте изложения, выстроены в логической последовательности, иллюстрированные конкретными примерами, изложены грамотным экономическим языком, свидетельствующим об овладении специальной терминологией и свободном понимании, и владении понятиями. На возникшие у преподавателя дополнительные вопросы студент должен давать четкие и конкретные ответы, показывая умение выделять существенные и несущественные моменты материала.

Оценка «незачтено» ставится, если при изложении ответов на теоретические вопросы даны неправильные ответы, свидетельствующие о том, что студент не усвоил понятия, у него не сформирован комплекс основных знаний по теме, в ответах отсутствует логика изложения, выводы, обобщения.

Разработчик  Е.А. Нечушкина