Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования «Ростовский государственный экономический университет (РИНХ)»

УТВЕРЖДАЮ
Директор Института магистратуры
_____ Иванова Е.А.
«29» 08 20 22 г.

Рабочая программа дисциплины
Математические и инструментальные методы обеспечения информационной безопасности

Направление 10.04.01 Информационная безопасность
магистерская программа 10.04.01.02 "Программно-аппаратные методы расследования компьютерных преступлений"

Для набора 2022 года

Квалификация
магистр

КАФЕДРА **Информационные технологии и защита информации**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	2 (1.2)		Итого	
Недель	15			
Вид занятий	УП	РП	УП	РП
Лекции	14	14	14	14
Практические	22	22	22	22
Итого ауд.	36	36	36	36
Контактная работа	36	36	36	36
Сам. работа	68	68	68	68
Часы на контроль	4	4	4	4
Итого	108	108	108	108

ОСНОВАНИЕ

Учебный план утвержден учёным советом вуза от 22.02.2022 протокол № 7.

Программу составил(и): д.э.н., проф., Тищенко Е.Н. _____

Зав. кафедрой: к.э.н., доцент Ефимова Е.В. _____

Методическим советом направления: д.э.н., проф., Тищенко Е.Н. _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	Овладение основными методами научного исследования; теоретическими основами компьютерной безопасности; формирование научного мировоззрения.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ПК-4:Способен осуществлять анализ результатов экспериментальных исследований с применением математических и физических методов, выбор технических средств инструментального мониторинга защищенности объектов информатизации

В результате освоения дисциплины обучающийся должен:

Знать:

формальные модели информационной безопасности объектов информатизации;
основные характеристики и показатели эффективности средств и систем обеспечения информационной безопасности;
источники и классификацию угроз информационной безопасности;
основные характеристики технических средств обеспечения информационной безопасности от утечек по техническим каналам;
методы обработки данных мониторинга информационной безопасности объектов информатизации;
порядок создания и структуру отчета, создаваемого по результатам исследования. (соотнесено с индикатором ПК-4.1.)

Уметь:

формализовать задачу обеспечения информационной безопасности объекта информатизации;
анализировать и прогнозировать критерии эффективности обеспечения информационной безопасности объекта информатизации;
классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности, оценивать угрозы информационной безопасности;
определять виды и типы технических средств обеспечения информационной безопасности; применять инструментальные средства мониторинга защищенности объекта информатизации;
структурировать аналитическую информацию для включения в отчет (соотнесено с индикатором ПК-4.2.)

Владеть:

навыками разработки модели информационной безопасности объекта информатизации;
навыками определения класса защищенности информационных систем;
навыками оценки критериев эффективности системы обеспечения информационной безопасности;
навыками подготовки аналитических отчетов по результатам проведенного анализа.(соотнесено с индикатором ПК-4.3.)

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература
	Раздел 1. Модели и методы обеспечения информационной безопасности				
1.1	Тема 1 "Основные положения теории информационной безопасности». Обоснование степени информационной безопасности проектируемых объектов информатизации. Обеспечение информационной безопасности при вводе объектов в эксплуатацию. Специальные проверки и специальные исследования. Оформление при помощи MS Office /Пр/	2	4	ПК-4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
1.2	1 "Основные положения теории информационной безопасности». Обоснование степени информационной безопасности проектируемых объектов информатизации. Обеспечение информационной безопасности при вводе объектов в эксплуатацию. /Лек/	2	2	ПК-4	Л1.1 Л1.2Л2.2 Л2.3
1.3	Построение систем защиты от угроз нарушения целостности информации: модель обеспечения целостности, криптографические методы. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. /Ср/	2	20	ПК-4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5

1.4	Тема 2 «Угрозы информационной безопасности. Теоретические основы построения систем защиты от угроз». Выбор и оптимизация требуемых мер и средств защиты информации на объектах. Аттестация объектов информатизации. Контроль за обеспечением безопасной эксплуатации объектов информатизации. Оформление при помощи MS Office /Пр/	2	6	ПК-4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
1.5	«Угрозы информационной безопасности. Теоретические основы построения систем защиты от угроз». Классификация угроз информационной безопасности. Построение систем защиты от угроз нарушения конфиденциальности информации: модель системы защиты, организационное обеспечение ИБ, идентификация и аутентификация, разграничение доступа, криптографические методы, контроль внешнего периметра, протоколирование, аудит. /Лек/	2	2	ПК-4	Л1.1 Л1.2Л2.1 Л2.3
1.6	Тема 2 «Угрозы информационной безопасности. Теоретические основы построения систем защиты от угроз». Классификация угроз информационной безопасности. Построение систем защиты от угроз нарушения конфиденциальности информации: модель системы защиты, организационное обеспечение ИБ, идентификация и аутентификация, разграничение доступа, криптографические методы, контроль внешнего периметра, протоколирование, аудит. /Ср/	2	20	ПК-4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
	Раздел 2. Методы и технологии информационной безопасности				
2.1	Методы нарушения конфиденциальности, целостности и доступности информации в условиях информационного противоборства. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны. Правовые, организационно-технические и экономические методы обеспечения ИБ. Модели, стратегии и системы обеспечения информационной безопасности в условиях информационного противоборства.LibreOffice /Пр/	2	6	ПК-4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
2.2	"Информационное противоборство, методы и средства его ведения. Методы и средства обеспечения информационной безопасности объектов информационной сферы». Информационное противоборство, информационная война. /Лек/	2	6	ПК-4	Л1.1 Л1.2Л2.5
2.3	Тема 1 "Информационное противоборство, методы и средства его ведения. Методы и средства обеспечения информационной безопасности объектов информационной сферы». Классификация возможных каналов утечки информации. Технологии зашиты акустической информации от утечки. Технологии зашиты информации от утечки по каналам ПЭМИН. Технологии зашиты видовой информации от утечки. /Ср/	2	8	ПК-4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
2.4	Тема 2 «Управление безопасностью в компьютерной системе». Классификация методов зашиты информации от программно-математических воздействий. Категорирование объектов информатизации. Деятельность администратора безопасности по предотвращению программно-математических воздействий. LibreOffice /Пр/	2	6	ПК-4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5

2.5	Тема 2 «Управление безопасностью в компьютерной системе». Термины и определения. Системы удаленного управления безопасности: в отсутствии локального объекта управления, при локальном объекте управления и удаленном управляющем объекте, при распределенном объекте управления. Модели воздействия внешнего злоумышленника на локальный сегмент компьютерной системы. /Ср/	2	20	ПК-4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
2.6	Деятельность администратора безопасности по минимизации последствий программно- математических воздействий. /Лек/	2	4	ПК-4	Л1.1 Л1.2 Л1.3Л2.4
2.7	/Зачёт/	2	4	ПК-4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Структура и содержание фонда оценочных средств для проведения текущей и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л1.1	Грушо А. А., Применко Э. А., Тимонина Е. Е.	Теоретические основы компьютерной безопасности: учеб. пособие для студентов вузов, обучающихся по спец. группы 090100 "Информ. безопасность"	М.: Академия, 2009	30
Л1.2	Ковалев Д. В., Богданова Е. А.	Информационная безопасность: учебное пособие	Ростов-на-Дону: Южный федеральный университет, 2016	https://biblioclub.ru/index.php?page=book&id=493175 неограниченный доступ для зарегистрированных пользователей
Л1.3	Шаньгин, В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019	http://www.iprbookshop.ru/87995.html неограниченный доступ для зарегистрированных пользователей

5.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Шейдаков Н. Е., Серпенинов О. В., Тищенко Е. Н.	Физические основы защиты информации: учеб. пособие для студентов высш. учеб. заведений, обучающихся по напр. подгот. "Информ. безопасность"	М.: РИО  , 2016	110
Л2.2	Рытенкова О.	Информационная безопасность: журнал	Москва: ГРОТЕК, 2013	https://biblioclub.ru/index.php?page=book&id=210607 неограниченный доступ для зарегистрированных пользователей
Л2.3		Информационное право и информационная безопасность. Часть 2: Учебник для магистров и аспирантов	Москва, Саратов: Всероссийский государственный университет юстиции (РПА Минюста России), Ай Пи Эр Медиа, 2016	http://www.iprbookshop.ru/66771.html неограниченный доступ для зарегистрированных пользователей

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.4		Информационное право и информационная безопасность. Часть 1: Учебник для магистров и аспирантов	Москва, Саратов: Всероссийский государственный университет юстиции (РПА Минюста России), Ай Пи Эр Медиа, 2016	http://www.iprbookshop.ru/72395.html неограниченный доступ для зарегистрированных пользователей
Л2.5	Катанова, Т. Н., Галкина, Л. С., Жданов, Р. А.	Информационная безопасность: лабораторный практикум	Пермь: Пермский государственный гуманитарно-педагогический университет, 2018	http://www.iprbookshop.ru/86357.html неограниченный доступ для зарегистрированных пользователей

5.3 Профессиональные базы данных и информационные справочные системы

СПС КонсультантПлюс

СПС Гарант

ЭБС «IPR Books» http://www.iprbookshop.ru/

Библиоклуб.ру http://biblioclub.ru/

5.4. Перечень программного обеспечения

LibreOffice

5.5. Учебно-методические материалы для студентов с ограниченными возможностями здоровья

При необходимости по заявлению обучающегося с ограниченными возможностями здоровья учебно-методические материалы предоставляются в формах, адаптированных к ограничениям здоровья и восприятия информации. Для лиц с нарушениями зрения: в форме аудиофайла; в печатной форме увеличенным шрифтом. Для лиц с нарушениями слуха: в форме электронного документа; в печатной форме. Для лиц с нарушениями опорно-двигательного аппарата: в форме электронного документа; в печатной форме.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Помещения для всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения:

- столы, стулья;

- персональный компьютер / ноутбук (переносной);

- проектор, экран / интерактивная доска.

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Методические указания по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

1 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

1.1 Показатели и критерии оценивания компетенций:

ЗУН, составляющие компетенцию	Показатели оценивания	Критерии оценивания	Средства оценивания
ПК-4: способен осуществлять анализ результатов экспериментальных исследований с применением математических и физических методов, выбор технических средств инструментального мониторинга защищенности объектов информатизации			
З. основные характеристики и показатели эффективности средств и систем обеспечения информационной безопасности; источники и классификацию угроз информационной безопасности; основные характеристики технических средств обеспечения информационной безопасности от утечек по техническим каналам; методы обработки данных мониторинга информационной безопасности объектов информатизации; порядок создания и структуру отчета, создаваемого по результатам исследования. (соотнесено с индикатором ПК-4.1.)	поиск и сбор необходимой литературы, использование различных баз данных	полнота и содержательность ответа умение приводить примеры	Т (тесты Раздел 1 тема 1 вопрос 1-2; Раздел 2 тема 1 вопрос 1), З (вопросы 1-4, 9-11, 25-26)
У. формализовать задачу обеспечения информационной безопасности объекта информатизации; анализировать и прогнозировать критерии эффективности обеспечения информационной безопасности объекта информатизации; классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности, оценивать угрозы информационной безопасности; определять виды и типы технических средств обеспечения информационной безопасности; применять инструментальные средства мониторинга защищенности объекта информатизации; структурировать аналитическую информацию для включения в отчет (соотнесено с индикатором ПК-4.2.)	использование информационных технологий в практической деятельности для приобретения новых знаний и умений	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	ПЗ (Раздел 1 практическое задание 1, часть 1) ПОЗЗ (1-6)
В. навыками разработки модели информационной безопасности объекта информатизации; навыками определения класса	использование современных информационно-коммуникационных	полнота и содержательность ответа умение приводить	ПЗ (Раздел 1 практическое задание 1, часть 2)

защищенности информационных систем; навыками оценки критериев эффективности системы обеспечения информационной безопасности; навыками подготовки аналитических отчетов по результатам проведенного анализа.(соотнесено с индикатором ПК-4.3.)	технологий и различных информационных ресурсов	примеры умение самостоятельно находить решение поставленных задач	ПОЗЗ (1-6)

ПЗ – практические задания, Т – тест, З – вопросы к зачету, ПОЗЗ- практико-ориентированные задания к зачету

1.2 Шкалы оценивания:

Текущий контроль успеваемости и промежуточная аттестация осуществляется в рамках накопительной балльно-рейтинговой системы в 100-балльной шкале.

- 50-100 баллов (зачет);
- 0-49 баллов (незачет).

2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Вопросы к зачету

1. Обеспечение информационной безопасности при вводе объектов в эксплуатацию.
2. Специальные проверки и специальные исследования.
3. Информационная безопасность: основные определения.
4. Понятие конфиденциальности, целостности, доступности информации.
5. Формальные модели управления доступом: модель Харрисона-Руззо-Ульмана, модель Белла Ла-Падулы. Формальные модели целостности: модель Кларка-Вилсона, модель Биба.
6. Совместное использование моделей безопасности.
7. Ролевое управление доступом.
8. Выбор и оптимизация требуемых мер и средств защиты информации на объектах.
9. Аттестация объектов информатизации.
10. Контроль за обеспечением безопасной эксплуатации объектов информатизации.
11. Теоретические основы построения систем защиты от угроз».
12. Классификация угроз информационной безопасности.
13. Построение систем защиты от угроз нарушения конфиденциальности информации: модель системы защиты, организационное обеспечение ИБ, идентификация и аутентификация, разграничение доступа, криптографические методы, контроль внешнего периметра, протоколирование, аудит.
14. Построение систем защиты от угроз нарушения целостности информации: модель обеспечения целостности, криптографические методы.
15. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.
16. Информационное противоборство, информационная война.
17. Методы нарушения конфиденциальности, целостности и доступности информации в условиях информационного противоборства.
18. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны.
19. Правовые, организационно-технические и экономические методы обеспечения ИБ.
20. Модели, стратегии и системы обеспечения информационной безопасности в условиях информационного противоборства.
21. Классификация возможных каналов утечки информации.
22. Технологии зашиты акустической информации от утечки.
23. Технологии зашиты информации от утечки по каналам ПЭМИН.
24. Технологии зашиты видовой информации от утечки.
25. Классификация методов зашиты информации от программно-математических воздействий.
26. Категорирование объектов информатизации.
27. Деятельность администратора безопасности по предотвращению программно-математических воздействий.

28. Деятельность администратора безопасности по минимизации последствий программно-математических воздействий.

29. Системы удаленного управления безопасности: в отсутствии локального объекта управления, при локальном объекте управления и удаленном управляющем объекте, при распределенном объекте управления.

30. Модели воздействия внешнего злоумышленника на локальный сегмент компьютерной системы.

31.

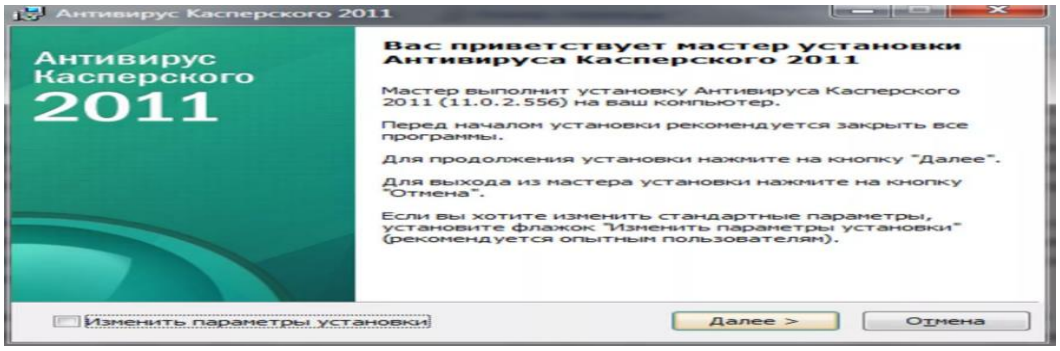
Практико-ориентированные задания к зачету

1. Установить угрозы, атаки и риски сетевой безопасности.
2. Установить антивирусное программное обеспечение.
3. Установить Linux-подобную операционную систему.
4. Настроить впервые установленную Linux-подобную операционную систему.
5. Установить шифровальную систему.

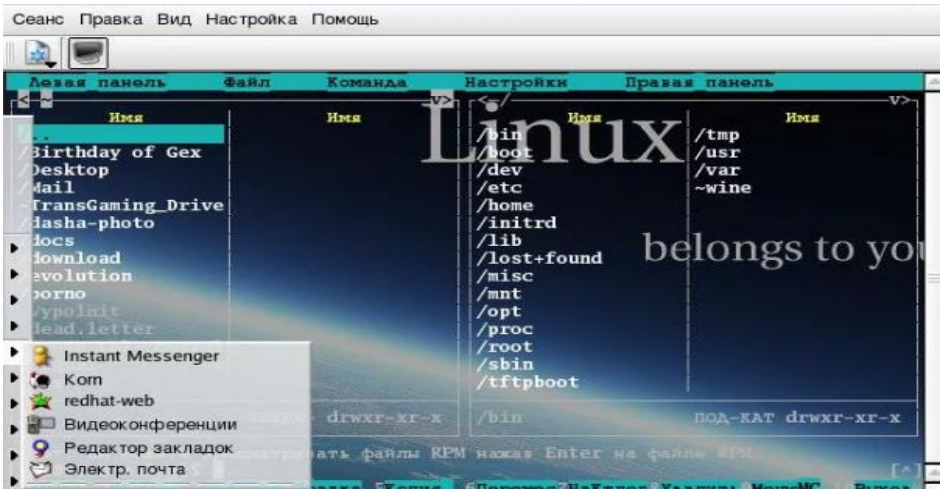
Ключ для контроля правильности выполнения практических заданий к экзамену

Установить угрозы, атаки и риски сетевой безопасности:

Установить антивирусное программное обеспечение:



Установить и настроить Linux-подобную операционную систему.



Установить шифровальную систему.

Критерии оценивания:

- 50-100 баллов (зачтено) – наличие твердых знаний в объеме пройденного курса в соответствии с целями обучения, изложение ответов с отдельными ошибками, уверенно исправленными после дополнительных вопросов; правильные в целом действия по применению знаний на практике;

- 0-49 баллов (Не зачтено) – ответы не связаны с вопросами, наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

Тесты

1. Банк тестов по модулям и (или) темам

Раздел 1 Модели и методы обеспечения информационной безопасности

Тема 1 " Основные положения теории информационной безопасности "

1. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

а) сотрудники
б) хакеры
в) атакующие
г) контрагенты (лица, работающие по договору)

2. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

а) владельцы данных
б) пользователи
в) администраторы
г) руководство

3. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

а) поддержка высшего руководства
б) эффективные защитные меры и методы их внедрения
в) актуальные и адекватные политики и процедуры безопасности
г) проведение тренингов по безопасности для всех сотрудников

Тема 2 " Угрозы информационной безопасности. Теоретические основы построения систем защиты от угроз».

1. Что такое политики безопасности?

а) инструкции по выполнению задач безопасности
б) общие руководящие требования по достижению определенного уровня безопасности
в) широкие, высокоуровневые заявления руководства
г) детализированные документы по обработке инцидентов безопасности

2. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

а) анализ рисков
б) анализ затрат / выгоды
в) результаты ALE
г) выявление уязвимостей и угроз, являющихся причиной риска

3. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

а) анализ рисков
б) анализ затрат / выгоды

в) результаты ALE
г) выявление уязвимостей и угроз, являющихся причиной риска

Раздел 2. Методы и технологии информационной безопасности

Тема 1. «Информационное противоборство, методы и средства его ведения. Методы и средства обеспечения информационной безопасности объектов информационной сферы».

1. Для решения каких задач предназначены статические оболочки экспертных систем?
a) для управления и диагностики в режиме реального времени
b) для решения статических задач
c) для решения задач анализа и синтеза с разделением времени
d) для разработки динамических систем
e) нет правильного ответа

2. Эффективная программа безопасности требует сбалансированного применения:
а) технических и нетехнических методов
б) контрмер и защитных механизмов
в) физической безопасности и технических средств защиты
г) процедур безопасности и шифрования

3. Что из перечисленного не является целью проведения анализа рисков?
а) делегирование полномочий
б) количественная оценка воздействия потенциальных угроз
в) выявление рисков
г) определение баланса между воздействием риска и стоимостью необходимых контрмер

Тема 2. «Управление безопасностью в компьютерной системе».

1.Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?
а) поддержка
б) выполнение анализа рисков
в) определение цели и границ
г) делегирование полномочий

2. Целостность и наглядность описания предметной области сохраняется в семантических сетях с увеличением размеров и усложнением связей
a) да
b) нет

3.Задачи аппаратного моделирования деятельности человека могут относиться к задачам искусственного интеллекта
a) да
b) нет

Тестовое задание выполняется на отдельном листе. Лист подписывается ФИО, номер группы, номер зачетной книжки, указывается вариант тестового задания. Ниже обучающийся указывает цифрой номер вопроса и рядом ставит номер правильного, на его взгляд, варианта ответа. Тестовое задание содержит 10 вопросов с вариантами ответов. Если обучающийся до сдачи преподавателю тестового задания и листа с ответами, считает, что не правильно ответил на тот или иной вопрос теста, то зачеркивает предыдущий вариант ответа и рядом указывает новый. За ошибку это не считается. Время прохождения тестирования 20 минут. После окончания выполнения тестового задания обучающийся сдает преподавателю вариант тестового задания и лист с ответами.

3. Критерии оценки:

- 1-20 баллов выставляется обучаемому. За один правильный ответ обучаемый получает 2 балла.

Практические задания

1.Тематика практических заданий по разделам и темам

Раздел 1 «**Модели и методы обеспечения информационной безопасности**»

Тема 1 «Основные положения теории информационной безопасности»

Практическое задание 1 Обоснование степени информационной безопасности проектируемых объектов информатизации. Обеспечение информационной безопасности при вводе объектов в эксплуатацию. Специальные проверки и специальные исследования. Оформление при помощи MS Office.

Тема 2 «Угрозы информационной безопасности. Теоретические основы построения систем защиты от угроз».

Практическое задание 2. Выбор и оптимизация требуемых мер и средств защиты информации на объектах. Аттестация

объектов информатизации. Контроль за обеспечением безопасной эксплуатации объектов информатизации. Оформление при помощи MS Office.

Раздел 2. «**Методы и технологии информационной безопасности**».

Тема 1. «Информационное противоборство, методы и средства его ведения. Методы и средства обеспечения информационной безопасности объектов информационной сферы».

Практическое задание 1 Информационное противоборство, информационная война. Методы нарушения конфиденциальности, целостности и доступности информации в условиях информационного противоборства. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны. Правовые, организационно-технические и экономические методы обеспечения ИБ. Модели, стратегии и системы обеспечения информационной безопасности в условиях информационного противоборства.

Тема 2. «Управление безопасностью в компьютерной системе».

Практическое задание 2. Классификация методов зашиты информации от программно-математических воздействий. Категорирование объектов информатизации. Деятельность администратора безопасности по предотвращению программно-математических воздействий. Деятельность администратора безопасности по минимизации последствий программно-математических воздействий.

Критерии оценки:

- (для каждого задания):

20 б. – задание выполнено верно;

19-15 б. – при выполнении задания были допущены неточности, не влияющие на результат;

14-10 б. – при выполнении задания были допущены ошибки;

9 - 1 б. – при выполнении задания были допущены существенные ошибки;

0 б. – задание не выполнено.

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

Процедуры оценивания включают в себя текущий контроль и промежуточную аттестацию.

Текущий контроль успеваемости проводится с использованием оценочных средств, представленных в п. 2 данного приложения. Результаты текущего контроля доводятся до сведения студентов до промежуточной аттестации.

Зачет проводится по расписанию промежуточной аттестации.

Количество вопросов в задании – 3. Объявление результатов производится в день зачета. Результаты аттестации заносятся в зачетную ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику, должны ликвидировать задолженность в установленном порядке.

Приложение 2

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Учебным планом предусмотрены следующие виды занятий:

- лекции;
- практические занятия.

В ходе лекционных занятий рассматриваются основные теоретические вопросы по дисциплине.

В ходе практических занятий углубляются и закрепляются знания студентов по ряду рассмотренных вопросов, развиваются навыки комплексной оценки безопасности автоматизированных информационных и телекоммуникационных систем.

Вопросы, не рассмотренные на лекционных и практических занятиях, должны быть изучены студентами в ходе самостоятельной работы. Контроль самостоятельной работы студентов над учебной программой курса осуществляется в ходе занятий методом устного опроса или посредством тестирования. В ходе самостоятельной работы каждый студент обязан прочитать основную и по возможности дополнительную литературу по изучаемой теме, дополнить конспекты лекций недостающим материалом, выписками из рекомендованных первоисточников. Выделить непонятные термины, найти их значение в энциклопедических словарях.

Студент должен готовиться к предстоящему лекционному и практическому занятию по всем, обозначенным в рабочей программе дисциплины вопросам.

Для подготовки к занятиям, текущему контролю и промежуточной аттестации студенты могут воспользоваться электронно-библиотечными системами. Также обучающиеся могут взять на дом необходимую литературу на абонементе университетской библиотеки или воспользоваться читальными залами.