МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«УФИМСКИЙ ГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра *Вычислительной техники и защиты информации*

УТВЕРЖДАЮ

Первый проректор по науке

_____Р.Д. Еникеев

«_23_» _____июня_____2022 г.

РАБОЧАЯ ПРОГРАММА

УЧЕБНОЙ ДИСЦИПЛИНЫ

«*МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ*»

Уровень подготовки
высшее образование - подготовка научных и научно-педагогических кадров в аспирантуре

Научная специальность

2.3.6 Методы и системы защиты информации, информационная безопасность

Квалификация (ученая степень): кандидат наук

Форма обучения
очная

Уфа 2022

Рабочая программа учебной дисциплины «*Методы и системы защиты информации, информационная безопасность*»

Рабочая программа дисциплины обсуждена на заседании кафедры ВТиЗИ 08.04.2022 г., протокол № 11 и рекомендована к реализации в образовательном процессе для подготовки аспирантов по ПА2.3.6 «Методы и системы защиты информации, информационная безопасность».

Заведующий кафедрой: _____ В.М.Картак

Составитель: _____ В.В. Сагитова, к.т.н., старший преподаватель кафедры ВТиЗИ

Согласовано: _____ Р.К. Фаттахов, к.т.н., доцент, начальник ОАиД

Оглавление

1. Место дисциплины в структуре образовательной программы

Дисциплина «Методы и системы защиты информации, информационная безопасность» является дисциплиной, направленной на подготовку к сдаче кандидатских экзаменов, образовательного компонента программы аспирантуры подготовки научных и научно-исследовательских кадров в аспирантуре по научной специальности 2.3.6 Методы и системы защиты информации, информационная безопасность.

Рабочая программа составлена в соответствии с Федеральными государственными требованиями к структуре программам подготовки научных и научно-педагогических кадров в аспирантуре (адъюнктуре)», утвержденных приказом Министерства науки и высшего образования Российской Федерации (Минобрнауки России) от 20 октября 2021 года № 951; Постановление Правительства Российской Федерации от 30.11.2021 № 2122 "Об утверждении Положения о подготовке научных и научно-педагогических кадров в аспирантуре (адъюнктуре)".

Является неотъемлемой частью программы аспирантуры подготовки научных и научно-исследовательских кадров в аспирантуре. Дисциплина направлена на подготовку к сдаче кандидатского экзамена.

Целью освоения дисциплины является ознакомление с комплексом проблем информационной безопасности предпринимательских структур различных типов и направлений деятельности, построения и функционирования совокупности правовых, организационных, технических и технологических процессов, обеспечивающих информационную безопасность и формирующих структуру системы защиты ценной и конфиденциальной информации в сферах охраны интеллектуальной собственности предпринимателей и сохранности их информационных ресурсов.

Задачи:

а) овладение теоретическими, практическими и методическими вопросами классификации угроз информационным ресурсам;

б) ознакомление с современными проблемами информационной безопасности, основными концептуальными положениями системы защиты информации;

в) изучение основных направлений обеспечения информационной безопасности, меры законодательного, административного, процедурного и программно-технического уровней при работе на вычислительной технике и в каналах связи;

г) приобретение теоретических и практических навыков по использованию современных методов защиты информации в компьютерных системах;

д) формирование практических навыков и способностей осуществления мероприятий по обеспечению информационной безопасности функционирования информационной системы при взаимодействии с информационными рынками по сетям или с использованием иных методов обмена данными.

2. Содержание и структура дисциплины (модуля)

Общая трудоемкость дисциплины составляет 3 зачетных единиц (108 часов).

Трудоемкость дисциплины по видам работ

Вид работы	Трудоемкость, час.
	3 курс, 5 семестр
Лекции (Л)	10
Практические занятия (ПЗ)	
Лабораторные работы (ЛР)	
КСР	1
Курсовая проект работа (КР)	

Расчетно - графическая работа (РГР)	
Самостоятельная работа (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, коллоквиумам, рубежному контролю и т.д.)	61
Подготовка и сдача экзамена	36
Подготовка и сдача зачета	
Вид итогового контроля (зачет, экзамен)	экзамен

Содержание разделов и формы текущего контроля

№	Наименование и содержание раздела	Количество часов						Литература, рекомендуемая аспирантам*
		Аудиторная работа				СРС	Всего	
		Л	ПЗ	ЛР	КСР			
1	**Концепция информационной безопасности**: – Актуальность информационной безопасности. – Лицензирование и сертификация в области защиты информации. – Основные нормативные руководящие документы.	2				11	13	2, 4, 5
2	**Угрозы информации**: – Информационная безопасность сетей. – Способы совершения компьютерных преступлений. – Уязвимость сети Интернет.	2				10	12	2, 3, 5, 7, 8
3	**Виды возможных нарушений безопасности информационной системы**: – Компьютерные преступления. – Вредоносные программы. – Вирусы.	2				10	12	2, 4, 5, 10
4	**Информационная безопасность информационных систем**: – Теория информационной безопасности информационных систем. – Криптографические способы защиты информации. – Организация информационной безопасности компании.	2			1	10	13	2, 3, 4, 7
5	**Методы и средства защиты компьютерной информации**: – Обеспечение информационной безопасности. – Контроль доступа к информации. – Методы и средства защиты информации. – Антивирусное ПО.	2				20	22	1, 2, 6, 7, 8, 9

3. Учебно-методическое обеспечение самостоятельной работы аспирантов

Тема 1. Концепция информационной безопасности.

Вопросы для самостоятельного изучения (подготовке к обсуждению):

1. Компьютерные преступления, законодательные и нормативные документы.
2. Правила функционирования системы лицензирования.
3. Правовое обеспечение защиты информации в России и за рубежом.
4. Руководящие документы Гостехкомиссии.
5. Международные стандарты информационного обмена.
6. Критерии безопасности компьютерных систем. «Оранжевая книга».
7. Правовое регулирование защиты персональных данных в РФ.

Тема 2. Угрозы информации.

Вопросы для самостоятельного изучения:

1. Угрозы безопасности информации и их классификация.
2. Государственная система защиты информации, обрабатываемая техническими средствами.
3. Требования к защите информации, оценка возможностей противоборствующей стороны.
4. Методология разработки и анализа средств защиты.
5. Классические модели защиты информации.
6. Причины уязвимости сети Интернет. Удаленные атаки на интрасети.

Тема 3. Виды возможных нарушений безопасности информационной системы.

Вопросы для самостоятельного изучения:

1. Обобщенная структура IP-сети. Сетевые ресурсы.
2. Классы каналов связи. Основы IP-адресации и маршрутизации.
3. Технические и программные средства сетевой передачи данных и сегментации сети.
4. Характеристика объекта информатизации (выделенного помещения), как объекта защиты от технических разведок.
5. Цели и задачи защиты информации от утечки по техническим каналам (технической защиты информации).
6. Характеристики и классификация технических каналов утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами.
7. Исследование параметров радиоканала системы перехвата речевой информации.
8. Основные технические характеристики средств акустической разведки. Методика применения средств акустической разведки.
9. Разновидности вредоносных программ.

Тема 4. Информационная безопасность информационных систем.

Вопросы для самостоятельного изучения:

1. Способы восстановления работоспособности операционных систем.
2. Резервное копирование и восстановление данных.
3. Аварийное восстановление системы.
4. Аппаратные и механические средства защиты ПЭВМ.

5. Электронные ключи.

6. Аппаратный модуль доверенной загрузки «Соболь»

7. Обзор средств криптографической защиты конфиденциальной информации.

8. Изучение стандартов шифрования AES и Rijndael

9. Настройка криптографических функций. Работа с ключевой информацией.

10. Фильтры. Стратегии формирования фильтров

11. Трансляция адресов (NAT). Настройка NAT-обработчика.

Тема 5. Методы и средства защиты компьютерной информации.

Вопросы для самостоятельного изучения:

1. Механизм защиты входа в систему.

2. Полномочное и избирательное разграничение доступа.

3. Организационные вопросы защиты программ и данных компьютерных систем и сетей.

4. Цели, функции и задачи защиты информации в сетях ЭВМ.

5. Современные средства обеспечения информационной безопасности вычислительных сетей.

6. Сканеры безопасности.

7. Защита от внешних атак.

8. Внутренняя безопасность.

9. Понятие электронной подписи.

10. Взаимосвязь между протоколами аутентификации и электронной подписи.

11. Хэш - функция и ее использование в системах электронной подписи. Схемы ЭП.

4. Фонд оценочных средств

Оценка уровня освоения дисциплины осуществляется в виде текущего и промежуточного контроля успеваемости аспирантов университета, и на основе критериев оценки уровня освоения дисциплины.

Активность обучающегося оценивается на занятиях и на основе выполненных работ и заданий, предусмотренных ФОС дисциплины.

Оценивание проводится преподавателем независимо от наличия или отсутствия обучающегося (по уважительной или неуважительной причине) на занятии. Оценка носит комплексный характер и учитывает достижения обучающегося по основным компонентам образовательного процесса за текущий период.

№ п/п	Контролируемые разделы (темы) дисциплины	Наименование оценочного средства*
1	Концепция информационной безопасности.	Собеседование, комплексное задание, ответы на вопросы
2	Угрозы информации.	Собеседование, комплексное задание, ответы на вопросы
3	Виды возможных нарушений безопасности информационной системы.	Собеседование, комплексное задание, ответы на вопросы
4	Информационная безопасность информационных систем.	Собеседование, комплексное задание ,ответы на вопросы

5	Методы и средства защиты компьютерной информации.	Собеседование, комплексное задание, ответы на вопросы

Вопросы к экзамену

1. Законодательные и правовые основы защиты компьютерной информации информационных технологий.
2. Безопасность информационных ресурсов и документирование информации.
3. персональные данные о гражданах.
4. Вычислительные сети и защита информации; нормативно-правовая база функционирования систем защиты информации.
5. Российское законодательство по защите информационных технологий.
6. Правовая защита программного обеспечения авторским правом.
7. Проблемы защиты информации в информационных системах.
8. Меры по обеспечению сохранности информации и угрозы ее безопасности в информационных системах.
9. защита локальных сетей и операционных систем.
10. Internet в структуре информационно-аналитического обеспечения информационных систем; рекомендации по защите информации в Internet.
11. Содержание системы средств защиты компьютерной информации в информационных системах.
12. Защищенная информационная система и система защиты информации.
13. Законодательная, нормативно-методическая и научная база системы защиты информации.
14. Требования к содержанию нормативно-методических документов по защите информации.
15. Организационно-правовой статус службы информационной безопасности; организационно-технические и режимные меры.
16. Политика безопасности.
17. Программно-технические методы и средства защиты информации.
18. Программно-аппаратные методы и средства ограничения доступа к компонентам компьютера.
19. Типы несанкционированного доступа и условия работы средств защиты.
20. Симметричные криптосистемы: основные понятия и определения.
21. Применение симметричных криптосистем для защиты компьютерной информации в информационных системах.
22. Изучение американского стандарта шифрования данных DES.
23. Отечественный стандарт шифрования данных; режим простой замены.
24. Режим гаммирования; режим гаммирования с обратной связью.
25. Режим выработки имитовставки; блочные и поточные шифры.
26. Применение асимметричных криптосистем для защиты компьютерной информации в информационных системах.
27. Концепция криптосистемы с открытым ключом.
28. Криптосистема шифрования данных RSA (процедуры шифрования и расшифрования в этой системе).
29. Схема шифрования Полига—Хеллмана.
30. Схема шифрования Эль-Гамаля.
31. Методы идентификации и проверки подлинности пользователей компьютерных систем. проблема аутентификации данных и электронная подпись.
32. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов.
33. Отечественный стандарт хэш-функции.
34. Алгоритм цифровой подписи RSA.
35. Алгоритм цифровой подписи Эль-Гамаля (EGSA).
36. Алгоритм цифровой подписи DSA.

37. Отечественный стандарт цифровой подписи.
38. Защита компьютерных систем от удаленных атак через сеть Internet.
39. Изучение существующих аппаратно-программных средств криптографической защиты компьютерной информации серии КРИПТОН.
40. Программно-аппаратная система защиты от несанкционированного доступа (НСД) КРИПТОН-ВЕТО.
41. Защита от НСД со стороны сети; абонентское шифрование и ЭП.
42. Методы защиты программ от изучения и разрушающих программных воздействий (программных закладок и вирусов).
43. Классификация способов защиты; защита от отладок и дизассемблирования.
44. Способы встраивания защитных механизмов в программное обеспечение.
45. Комплексная защита процесса обработки информации в компьютерных системах на основе стохастической интеллектуальной информационной технологии.
46. Метод защиты от НСД и разрушающих программных воздействий процесса хранения, обработки информации; защита арифметических вычислений в компьютерных системах.
47. Список практических вопросов и задач на экзамене по дисциплине.
48. Алгоритмы шифрования последовательности блоков методами DES, ГОСТ 28147-89 во всех режимах.
49. Алгоритмы многораундового шифрования блока методами DES, ГОСТ 28147-89 во всех режимах.
50. Операции, применяемые для шифрования блока в раунде методами DES, ГОСТ 28147-89.
51. Алгоритмы шифрования блока в раунде методами DES, ГОСТ 28147-89.
52. Алгоритмы выработки ключа для шифрования блока в раунде методами DES, ГОСТ 28147-89.
53. Операции в конечном поле GF(28) (умножение, сложение и т.д.).
54. Алгоритм многораундового шифрования методом Rijndael.
55. Алгоритм раундового преобразования при шифровании Rijndael.
56. Операции раундового преобразования и их реализация.
57. Алгоритм выработки раундовых ключей при шифровании Rijndael.
58. Выработка открытого ключа для шифрования алгоритмом RSA. Алгоритм шифрования и подписывания методом RSA.
59. Определение секретного ключа по открытому ключу в алгоритме RSA. Алгоритмы определения взаимной простоты чисел (e и n) и поиска обратного элемента e-1 mod n.
60. Алгоритм поиска примитивных элементов в поле GF(P). Алгоритм Диффи-Хэллмана выработки общего секретного ключ.

Задачи на экзамене

1. Выработать открытый ключ для шифрования алгоритмом RSA.
2. Зашифровать и подписать открытый текст (ОТ) методом RSA.
3. Определить секретный ключ по открытому ключу в алгоритме RSA.
4. Определить взаимную простоту чисел (e и n) и найти обратный элемент e-1 mod n.
5. Найти (доказать примитивность) примитивный элемент в поле GF(P).
6. Выработать общий секретный ключ по алгоритму Диффи-Хэллмана.
7. Методы поиска и сбора информации.
8. Методика устранения компьютерной информации.
9. Уязвимости Windows.
10. Уязвимости UNIX
11. Защита от копирования переносных носителей.
12. Аппаратные ключи защиты.
13. Современные криптосистемы.
14. Виды шифров. Методика кодирования.
15. Антивирусное программное обеспечение.

16. Особенности защиты информации при работе в сети.
17. Безопасная работа в Internet.
18. Целесообразность усиления обороны.
19. Защита от побочного электромагнитного излучения и наводок.
20. Алгоритмы распределения ключей.

Критерии оценки:

- оценка «отлично» выставляется аспиранту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал различной литературы, правильно обосновывает принятое нестандартное решение, владеет разносторонними навыками и приемами выполнения практических задач по формированию общепрофессиональных компетенций;
- оценка «хорошо» выставляется аспиранту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения, а также имеет достаточно полное представление о значимости знаний по дисциплине;
- оценка «удовлетворительно» выставляется аспиранту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает сложности при выполнении практических работ и затрудняется связать теорию вопроса с практикой;
- оценка «неудовлетворительно» выставляется аспиранту, который не знает значительной части программного материала, неуверенно отвечает, допускает серьезные ошибки, не имеет представлений по методике выполнения практической работы. Как правило, оценка «неудовлетворительно» ставится аспирантам, которые не могут продолжить обучение без дополнительных занятий по данной дисциплине.

Типовые оценочные материалы

1) Вопросы для собеседования.

Тема 1. Концепция информационной безопасности:

1. Критерии безопасности компьютерных систем.
2. Международные стандарты информационной безопасности.
3. Общие принципы построения защищенных информационных систем
4. Средства разработки ИС и правила их реализации.
5. Защищенные информационные технологии.

2) Тестирование

Тема 2. Угрозы информации.

Примеры вопросов тестов.

Задание 1. В каком году в России появились первые преступления с использованием компьютерной техники (были похищены 125,5 тыс. долл. США во Внешэкономбанке)?

1. 1988;
2. 1991;
3. 1994;
4. 1997;
5. 2002.

Задание 2. Сертификации подлежат:

1. средства криптографической защиты информации;
2. средства выявления закладных устройств и программных закладок;
3. защищенные технические средства обработки информации;
4. защищенные информационные системы и комплексы телекоммуникаций;
5. все вышеперечисленные средства.

Задание 3. В стандарте США «Оранжевой книге» фундаментальное требование, которое относится к группе Стратегия:

1. индивидуальные субъекты должны идентифицироваться;
2. контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность;
3. необходимо иметь явную и хорошо определенную систему обеспечения безопасности;
4. вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенных требований;
5. гарантированно защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взлома» и/или несанкционированного внесения изменений.

Задание 4. Естественные угрозы безопасности информации вызваны:

1.деятельностью человека;
2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
3. воздействиями объективных физических процессов или стихийных природных явлений, не зависящих от человека;
4. корыстными устремлениями злоумышленников;
5. ошибками при действиях персонала.

Задание 5. Хакер – это:
1. лицо, которое взламывает интрасеть в познавательных целях;
2. мошенник, рассылающий свои послания в надежде обмануть наивных и жадных;
3. лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов, разрушающих ПО;
4. плохой игрок в гольф, дилетант;
5. мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.
Задание 6. Активный перехват информации это – перехват, который:
1. заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
2. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
3. неправомерно использует технологические отходы информационного процесса;
4. осуществляется путем использования оптической техники;
5. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.
Задание 7. Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:
1. черный пиар;
2. фишинг;
3. нигерийские письма;
4. источник слухов;
5. пустые письма.
Задание 8. По среде обитания классические вирусы разделяются:
1. на паразитические;
2. на компаньоны;
3. на файловые;
4. на ссылки;
5. на перезаписывающие.
Задание 9. Шифрование методом подстановки:
1. символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста;
2. символы шифруемого текста последовательно складываются символами некоторой специальной последовательности;
3. шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор;
4. символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов;
5. замена слов и предложений исходной информации шифрованными.
Задание 10. Метод защиты информации ограничение доступа заключается:
1. в контроле доступа к внутреннему монтажу, линиям связи и технологическим органам управления;
2. в создании физической замкнутой преграды с организацией доступа лиц, связанных с объектом функциональными обязанностями;

3. в разделении информации на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями;
4. в том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы;
5. в проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.
Задание 11. Перехват, который неправомерно использует технологические отходы информационного процесса, называется:
1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.
Задание 12. Спам, периодически проводящий рассылки не рекламных сообщений:
1. черный пиар;
2. фишинг;
3. нигерийские письма;
4. источник слухов;
5. пустые письма.
Задание 13. Способ защиты информации, существующей в виде электромагнитного сигнала, зависит от …
1. среды распространения электромагнитного сигнала;
2. длины волны сигнала;
3. наличия или отсутствия специальной линии связи;
4. типа линии связи;
5. форм воздействия на информацию или ее носитель;
6. предполагаемого способа нападения на информацию.
Задание 14. Попытка одного субъекта выдать себя за другого - это:
1. пассивная атака;
2. модификация потока данных»
3. фальсификация;
4. повторное использование;
5. отказ в обслуживании.
Задание 15. Антивирус просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок:
1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

Критерии оценки:
- оценка «зачтено» выставляется аспиранту, если процент правильных ответов не менее 61%;
- оценка «не зачтено» выставляется аспиранту, если процент правильных ответов менее 61%.

3) Кейс-задача

Темы:

4 «Информационная безопасность информационных систем»

6 «Методы и средства защиты компьютерной информации»

Кейс – это пакет заданий, индивидуальных или групповых, которые очерчивают реальную проблему, не имеющую единственного и очевидного решения. Для поисков оригинального выхода аспирант должен проанализировать проблемную ситуацию, используя знания по изучаемой дисциплине, предложить решения и обосновать выбор именно этих вариантов. Применение кейс-метода позволяет развивать навыки работы с разнообразными источниками информации, а также компетентностные качества личности (аналитические, практические, творческие, коммуникативные, социальные умения).

Методика выполнения кейс-задания включает в себя следующие этапы: индивидуальная самостоятельная работа аспирантов с материалами кейса (идентификация проблемы, формулировка ключевых альтернатив, предложение решения или рекомендуемого действия); работа в малых группах по согласованию видения ключевой проблемы и ее решений; презентация и проверка результатов малых групп на общей дискуссии.

Примеры заданий

Задание 1. Необходимо построить защищенное соединение между двумя компьютерами. Приведите отчет с результатами выполнения и описанием произведенных действий. Архитектура защищенного канала может быть:

- сервер-клиент
- клиент-клиент

Задание 2. Необходимо настроить защищенный обмен между двумя пользователями при помощи криптографических и стеганографических контейнеров. Приведите отчет с результатами выполнения и описанием произведенных действий.

Задание 3. Необходимо построить централизованную инфраструктуру открытых ключей. Удостоверяющим центром являетесь вы. Необходимо создать не менее двух пользователей, а также сформировать список отозванных сертификатов. Приведите отчет с результатами выполнения и описанием произведенных действий.

Задание 4. Даны некоторые ценные документы. Необходимо их подписать с помощью цифровой подписи и подготовить их для передачи предварительно зашифровав. Приведите отчет с результатами выполнения и описанием произведенных действий.

Критерии оценки:

- оценка «зачтено» выставляется аспиранту, если он аргументировал выполнение задания, подтверждая знание материала, и сделал выводы по проделанной работе;
- оценка «не зачтено» - если задание не выполнено.

4) Типовые задания.

Тема 3. Виды возможных нарушений информационной системы.

Тема 5. Методы и средства защиты компьютерной информации

Вариант № 1 Организация криптографической защиты почтовых сообщений, а также сообщений передаваемых с помощью online-служб.
Вопросы:
1. В чем преимущество использования передачи зашифрованного сообщения
2. По какому алгоритму происходит шифрование данных?
3. Что такое электронная подпись (ЭП)?
4. Какой алгоритм используется в данной программе?
5. Назовите назначение использование ЭП?
6. В чем отличие ЭП от алгоритма шифрования?

Вариант № 2 Криптографические системы
Вопросы:
1. В чем преимущество использования передачи зашифрованного сообщения.
2. По какому алгоритму происходит шифрование данных?
3. Что такое электронная подпись (ЭП)?
4. Какой алгоритм используется в данной программе?
5. Назовите назначение использование ЭП?
6. В чем отличие ЭП от алгоритма шифрования?

Вариант № 3 Криптографическая защита информации от несанкционированного использования на персональных компьютерах, ноутбуках и сменных носителях
Вопросы:
1. В чем преимущество хранения данных в зашифрованном виде?
2. По какому алгоритму происходит шифрование данных?
3. Какие алгоритмы используется в данной программе?

Вариант № 4 Обеспечение информационной безопасности посредством разграничения доступа к ресурсам в операционной системе Windows
Вопросы:
1. Охарактеризуйте существующие модели разграничения доступа?
2. Перечислите плюсы и минусы существующих моделей разграничения доступа?
3. Создайте папку «исследование» и для ограниченного пользователя назначьте атрибут «только просмотр», локально.
4. Повторите тоже самое задание для сетевого варианта.

Вариант № 5 Формирование групповой политики информационной безопасности: Active Directory
Вопросы:
1. Сформируйте домен рабочей группы.
2. Сформируйте шаблон безопасности.

Вариант № 6 Программная виртуализация гостевой операционной системы на примере программного продукта Virtualbox
Вопросы:
1. Как монтировать раздел диска или CD-ROM?

2. Возможно ли внутри виртуальной машины запустить еще одну виртуальную машину?

Критерии оценки:

- оценка «зачтено» выставляется аспиранту, если была проявлена дискуссионная активность в собеседовании и задания выполнены без ошибок;
- оценка «не зачтено» - отсутствовала дискуссионная активность в собеседовании и/или задания выполнены с ошибками.

5. Учебно-методическое и информационное обеспечение дисциплины

5.1 Основная литература

1. Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401

2. Нестеров, С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров. — Санкт-Петербург : Лань, 2021. — 324 с. — ISBN 978-5-8114-6738-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com2/book/165837 .

3. Диогенес, Ю. Кибербезопасность. стратегия атак и обороны / Ю. Диогенес, Э. Озкайя ; перевод с английского Д. А. Беликова. — Москва : ДМК Пресс, 2020. — 326 с. — ISBN 978-5-97060-709-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/131717

4. Мельников В.П., под ред., Куприянов А.И. Информационная безопасность : Учебник / .— Электрон. дан. — Москва : КноРус, 2021 .— 267 с. Internet access .— URL:https://www.book.ru/book/939292

5. Прохорова, О. В., Информационная безопасность и защита информации [Электронный ресурс] : учебник / Прохорова О. В. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021 .— 124 с.—URL:https://e.lanbook.com/book/158939

6. Грибунин, В. Г. Комплексная система защиты информации на предприятии: учебное пособие для вузов / В. Г. Грибунин, В. В. Чудовский. – М.: Академия, 2009. – 411 с

7. Аверченков В. И. Организационная защита информации: учебное пособие для вузов 3-е изд., стер. - М.: Флинта, 2011. 224 с

5.2 Дополнительная литература

8. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : [учебное пособие] / В. Ф. Шаньгин .— Москва : Форум : Инфра-М, 2011.

9. Васильев В.И. Интеллектуальные системы защиты информации: учебное пособие / В.И. Васильев. 3-е изд.,испр., и доп.- М.:№Издательство "Инновационное машиностроение", 2017. - 201 с.

10. Дуленко, В. А. Уголовно-правовые, криминологические и криминалистические проблемы расследования преступлений в сфере высоких технологий и компьютерной информации / В. А. Дуленко, Р. Р. Мамлеев, В. А. Пестриков ; ГОУ ВПО УГАТУ .— Уфа : УГАТУ, 2009 .— 214 с. : ил. ; 21 см .— Библиогр.: с. 206-213 .— ISBN 978-5-86911-979-7.

5.3. Интернет-ресурсы (электронные учебно-методические издания, лицензионное программное обеспечение)

На сайте библиотеки http://library.ugatu.ac.ru/ в разделе «Информационные ресурсы», подраздел «Доступ к БД» размещены ссылки на интернет-ресурсы.

5.4 Методические указания к практическим занятиям

6. Адаптация рабочей программы для лиц с ОВЗ

При инклюзивном обучении лиц с ОЗВ предоставляется возможность использовать следующие материально-технические средства:

- для аспирантов с ОВЗ по зрению предусматривается применение средств преобразования визуальной информации в аудио и тактильные сигналы, таких как, брайлевская компьютерная техника, электронные лупы, видеоувеличители, программы невизуального доступа к информации, программы-синтезаторов речи;
- для аспирантов с ОВЗ по слуху предусматривается применение сурдотехнических средств, таких как, системы беспроводной передачи звука, техники для усиления звука, видеотехника, мультимедийная техника и другие средства передачи информации в доступных формах;

для аспирантов с нарушениями опорно-двигательной функции предусматривается применение специальной компьютерной техники с соответствующим программным обеспечением, в том числе, специальные возможности операционных систем, таких, как экранная клавиатура и альтернативные устройства ввода информации.