МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Факультет математики и компьютерных наук
Кафедра прикладной математики

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине
«Информационная безопасность»

Кафедра прикладной математики
факультета математики и компьютерных наук

Образовательная программа бакалавриата
01.03.05 – Статистика

Направленность (профиль) программы
Анализ больших данных

Форма обучения
Очная

Статус дисциплины:

Входит в часть, формируемая участниками образовательных отношений, модуль профильной направленности

Махачкала, 2023

Фонд оценочных средств по дисциплине «Информационная безопасность» составлена в 2023 году в соответствии с требованиями ФГОС ВО бакалавриата по направлению подготовки 01.03.05 - статистика от 14.08.2020 г. № 1032

Разработчики:

кафедра дискретной математики и информатики,

Алибеков Б.И. д.т.н., профессор;

Фонд оценочных средств по дисциплине «Информационная безопасность» одобрен: на заседании кафедры дискретной математики и информатики
от «20» 01 2023г.,
протокол № 5

Зав. кафедрой _____ Магомедов А.М

на заседании Методической комиссии факультета математики и компьютерных наук от
«25. 01.2023 г., протокол № 4.

Председатель _____ Ризаев М.К.

Фонд оценочных средств «Информационная безопасность» согласован с учебно-методическим управлением

«20» февраля 2023г. _____

1. ПАСПОРТ
ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине
«Информационная безопасность»

1.1.Основные сведения о дисциплине

Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 академических часов).

Вид работы	Трудоемкость, академических часов		
	6 семестр	___семестр	всего
Общая трудоёмкость	108		108
Контактная работа:	28		28
Лекции (Л)	14		14
Лабораторные занятия (ЛЗ)	14		14
Консультации			
Промежуточная аттестация (зачет, экзамен)	экзамен		16
Самостоятельная работа			
1. работа с лекционным материалом, с учебной литературой	6		6
2. опережающая самостоятельная работа (изучение нового материала до его изложения на занятиях)	8		8
3. выполнение домашних заданий, домашних контрольных работ	10		10
4. подготовка к лабораторным работам, к практическим и семинарским занятиям	10		10
5. подготовка к контрольным работам, коллоквиумам	10		10
6. подготовка к экзамену	36		36

1.2.Требования к результатам обучения по дисциплине, формы ихконтроля и виды оценочных средств

ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Информационная безопасность»

№п/п	Контролируемыемодули, разделы(темы) дисциплины	Код контролируемой компетенции (или её части)	Оценочные средства		Способ контроля
			наименование	№№ заданий	
1	Предмет, цели и задачи дисциплины “Информационная безопасность. Математические основы криптографии	УК-2	Вопросы для собеседования	1-7	устно
		ОПК-4	Тестовые задания	1-2	письменно
		УК-2 ОПК-4	Контрольные работы	1	письменно
2	Идентификация и аутентификация объектов сети. Средства антивирусной защиты.	УК-2 ОПК-4	Вопросы для собеседования	8-16	устно
		УК-2 ОПК-4	Тестовые задания	26-51	письменно
		УК-2 ОПК-4	Контрольные работы	2	письменно

1.3. Показатели и критерии определения уровня сформированности компетенций

№ п/п	Код компетенции	Уровни сформированности компетенции			
		Недостаточный	Удовлетворительный (достаточный)	Базовый	Повышенный
1	УК-2	Не знает на достаточном уровне : действующие правовые нормы в области научной и педагогической деятельности; имеющиеся ресурсы для разработки и реализации данного проекта. Не умеет на достаточном уровне: решать качественно и в срок круг задач, определяемых данным проектом. Не владеет на достаточном уровне: навыками решения конкретных задач с достижением поставленной цели в области научных исследований по математике и компьютерным наукам. Не знает на достаточном уровне : необходимые и (или) достаточные условия взаимосвязи вопросов и задач в различных областях математики; следственные связи между разными математическими утверждениями. Не умеет на достаточном уровне: выделять в рамках поставленных в проекте целей круг взаимосвязанных задач, который исходя из имеющихся ресурсов позволит реализовать данный проект. Не владеет на достаточном уровне: навыками выбора в рамках целей научных исследований круг взаимосвязанных математических задач, обеспечивающих достижение этих целей. Не знает на достаточном уровне : действующие правовые нормы в области научной и педагогической	Знает на достаточном уровне: действующие правовые нормы в области научной и педагогической деятельности; имеющиеся ресурсы для разработки и реализации данного проекта. Умеет на достаточном уровне : решать качественно и в срок круг задач, определяемых данным проектом. Владеет на достаточном уровне: навыками решения конкретных задач с достижением поставленной цели в области научных исследований по математике и компьютерным наукам. Знает на достаточном уровне: необходимые и (или) достаточные условия взаимосвязи вопросов и задач в различных областях математики; следственные связи между разными математическими утверждениями. Умеет на достаточном уровне : выделять в рамках поставленных в проекте целей круг взаимосвязанных задач, который исходя из имеющихся ресурсов позволит реализовать данный проект. Владеет на достаточном уровне: навыками выбора в рамках целей научных исследований круг взаимосвязанных математических задач,	Знает на хорошем уровне: действующие правовые нормы в области научной и педагогической деятельности; имеющиеся ресурсы для разработки и реализации данного проекта. Умеет на хорошем уровне : решать качественно и в срок круг задач, определяемых данным проектом. Владеет на хорошем уровне: навыками решения конкретных задач с достижением поставленной цели в области научных исследований по математике и компьютерным наукам. Знает на хорошем уровне: необходимые и (или) достаточные условия взаимосвязи вопросов и задач в различных областях математики; следственные связи между разными математическими утверждениями. Умеет на хорошем уровне : выделять в рамках поставленных в проекте целей круг взаимосвязанных задач, который исходя из имеющихся ресурсов позволит реализовать данный проект. Владеет на хорошем уровне: навыками выбора в рамках целей научных	Знает в совершенстве: действующие правовые нормы в области научной и педагогической деятельности; имеющиеся ресурсы для разработки и реализации данного проекта. Умеет в совершенстве: решать качественно и в срок круг задач, определяемых данным проектом. Владеет в совершенстве: навыками решения конкретных задач с достижением поставленной цели в области научных исследований по математике и компьютерным наукам. Знает в совершенстве: необходимые и (или) достаточные условия взаимосвязи вопросов и задач в различных областях математики; следственные связи между разными математическими утверждениями. Умеет в совершенстве: выделять в рамках поставленных в проекте целей круг взаимосвязанных задач, который исходя из имеющихся ресурсов позволит реализовать данный проект. Владеет в совершенстве: навыками выбора в

		деятельности. Не умеет на достаточном уровне: планировать этапы реализации данного проекта в области математических исследований с выбором оптимального способа его реализации. Не владеет на достаточном уровне: практическими навыками решения определенных задач в области научных исследований по прикладной математике и компьютерным наукам с применением нормативной базы.	обеспечивающих достижение этих целей. Знает на достаточном уровне: действующие правовые нормы в области научной и педагогической деятельности. Умеет на достаточном уровне : планировать этапы реализации данного проекта в области математических исследований с выбором оптимального способа его реализации. Владеет на достаточном уровне: практическими навыками решения определенных задач в области научных исследований по прикладной математике и компьютерным наукам с применением нормативной базы.	исследований круг взаимосвязанных математических задач, обеспечивающих достижение этих целей. Знает на хорошем уровне: действующие правовые нормы в области научной и педагогической деятельности. Умеет на хорошем уровне : планировать этапы реализации данного проекта в области математических исследований с выбором оптимального способа его реализации. Владеет на хорошем уровне: практическими навыками решения определенных задач в области научных исследований по прикладной математике и компьютерным наукам с применением нормативной базы.	рамках целей научных исследований круг взаимосвязанных математических задач, обеспечивающих достижение этих целей. Знает в совершенстве: действующие правовые нормы в области научной и педагогической деятельности. Умеет в совершенстве: планировать этапы реализации данного проекта в области математических исследований с выбором оптимального способа его реализации. Владеет в совершенстве: практическими навыками решения определенных задач в области научных исследований по прикладной математике и компьютерным наукам с применением нормативной базы.
2	ОПК-4	Не знает на достаточном уровне : прикладное современное программное обеспечение, применяемое в отрасли. Не умеет на достаточном уровне: применить прикладное современное программное обеспечение при решении практических задач. Не владеет на достаточном уровне: современным прикладным программным обеспечение, применяемое в отрасли. Не знает на достаточном уровне : выбрать и применить оптимальную прикладную программу для решения конкретной задачи.	Знает на достаточном уровне: прикладное современное программное обеспечение, применяемое в отрасли. Умеет на достаточном уровне : применить прикладное современное программное обеспечение при решении практических задач. Владеет на достаточном уровне: современным прикладным программным обеспечение, применяемое в	Знает на хорошем уровне: прикладное современное программное обеспечение, применяемое в отрасли. Умеет на хорошем уровне : применить прикладное современное программное обеспечение при решении практических задач. Владеет на хорошем уровне: современным прикладным программным обеспечение, применяемое в	Знает в совершенстве: прикладное современное программное обеспечение, применяемое в отрасли. Умеет в совершенстве: применить прикладное современное программное обеспечение при решении практических задач. Владеет в совершенстве: современным прикладным программным

		Не умеет на достаточном уровне: выбрать и применить оптимальную прикладную программу для решения конкретной задачи. Не владеет на достаточном уровне: методами выбора и применения оптимальной прикладной программы для решения конкретной задачи. . Не знает на достаточном уровне : навыки применения цифровых технологий для решения задач профессиональной деятельности. Не умеет на достаточном уровне: применить цифровые технология для решения задач профессиональной деятельности. систем и технологий. Не владеет на достаточном уровне: навыками применения цифровых технологий для решения задач профессиональной деятельности. уровне навыками сбора и обработки данных, полученными в области математических и (или) естественных наук, программирования и информационных технологий для формирования выводов по соответствующим научным исследованиям.	отрасли. Знает на достаточном уровне: выбрать и применить оптимальную прикладную программу для решения конкретной задачи. Умеет на достаточном уровне : выбрать и применить оптимальную прикладную программу для решения конкретной задачи. Владеет на достаточном уровне: методами выбора и применения оптимальной прикладной программы для решения конкретной задачи. . Знает на достаточном уровне: навыки применения цифровых технологий для решения задач профессиональной деятельности. Умеет на достаточном уровне : применить цифровые технология для решения задач профессиональной деятельности. систем и технологий. Владеет на достаточном уровне: навыками применения цифровых технологий для решения задач профессиональной деятельности.	отрасли. Знает на хорошем уровне: выбрать и применить оптимальную прикладную программу для решения конкретной задачи. Умеет на хорошем уровне : выбрать и применить оптимальную прикладную программу для решения конкретной задачи. Владеет на хорошем уровне: методами выбора и применения оптимальной прикладной программы для решения конкретной задачи. . Знает на хорошем уровне: навыки применения цифровых технологий для решения задач профессиональной деятельности. Умеет на хорошем уровне : применить цифровые технология для решения задач профессиональной деятельности. систем и технологий. Владеет на хорошем уровне: навыками применения цифровых технологий для решения задач профессиональной деятельности.	обеспечение, применяемое в отрасли. Знает в совершенстве: выбрать и применить оптимальную прикладную программу для решения конкретной задачи. Умеет в совершенстве: выбрать и применить оптимальную прикладную программу для решения конкретной задачи. Владеет в совершенстве: методами выбора и применения оптимальной прикладной программы для решения конкретной задачи. . Знает в совершенстве: навыки применения цифровых технологий для решения задач профессиональной деятельности. Умеет в совершенстве: применить цифровые технология для решения задач профессиональной деятельности. систем и технологий. Владеет в совершенстве: навыками применения цифровых технологий для решения задач профессиональной деятельности.

2.**КОНТРОЛЬНЫЕ ЗАДАНИЯ И ИНЫЕ МАТЕРИАЛЫ ОЦЕНКИ знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения дисциплины** «Информационная безопасность»

Контрольные работы

Контрольная работа 1

1.Дать определение информационной безопасности и охарактеризовать ее цели, задачи и структуру.
2.Определить место информационной безопасности в структуре информационного права.
3. Проанализировать современные проблемы информационной безопасности предпринимательской деятельности.
4. Описать порядок охраны информационных ресурсов открытого доступа.
5. Охарактеризовать порядок защиты информационных ресурсов ограниченного доступа.
6. Определить критерии ценности информационных ресурсов и длительности сохранения ими этой характеристики.

Варианты контрольных работ.

1. Номер варианта контрольной работы определяется по последней цифре номера зачетной книжки (или по последней цифре порядкового номера Ф.И.О. студента в списке журнала группы, если он взят за основу при определении варианта); цифра «10» означает вариант № 10.
Распределение теоретических вопросов по вариантам приведено в таблице1.

Таблица №1 – Распределение теоретических вопросов по вариантам

№ варианта	Номера вопросов				
1	1	11	21	31	41
2	2	12	22	32	42
3	3	13	23	33	43
4	4	14	24	34	44
5	5	15	25	35	45
6	6	16	26	36	46
7	7	17	27	37	47
8	8	18	28	38	48
9	9	19	29	39	49
10	10	20	30	40	50

1. Что такое информационная безопасность? Какие компоненты входят в информационную безопасность? Назовите пять этапов процесса информационной безопасности.
2. Почему безопасность – это процесс, а не конечный продукт?
3. Почему физическая защита не может гарантировать

безопасность?

4. Выделите два основных типа межсетевых экранов. От какого нападения защищают межсетевые экраны?

5. Назовите основные категории атак. Всегда ли атака модификации включает в себя атаку доступа?

6. Назовите основные категории атак. К какому типу атак особенно уязвимы беспроводные сети?

7. Что определяет политика безопасности? Почему в политику безопасности включают отказы от защиты?

8. Угрозы и их составляющие. Может ли угроза иметь более одной цели? Назовите четыре цели для угроз.

9. Что определяет политика безопасности? Назовите четыре необходимых политики безопасности.

10. Назовите основные категории атак. Каковы три вида атак на схему шифрования?

11. Назовите три типа аутентификационных факторов. Почему двухфакторная аутентификация сильнее, чем однофакторная?

12. Зачем нужен аудит? На какие три службы безопасности должен опираться аудит?

13. Что такое уязвимость? Основные виды уязвимостей и их отличия. Приведите несколько рекомендаций по устранению уязвимостей.

14. Назовите две составляющих риска. Каков уровень риска при отсутствии угроз?

15. Назовите ключевые концепции стандарта ISO, в котором говорится об информационной безопасности.

16. Может ли шифрование полностью защитить данные, передаваемые через VPN.

17. Какие механизмы аутентификации лучше всего использовать для пользовательской VPN?

18. Что подразумевается под пассивными ответными действиями? Что подразумевается под активными ответными действиями?

19. Каков приблизительный радиус действия беспроводной сети стандарта 802.11x на открытой местности и в помещении? Почему аутентификация 802.1X сама по себе рассматривается как уязвимость в системе?

20. К какому типу сетей следует относить WLAN? Какую периодическую оценку необходимо проводить при работе с WLAN?

21. Является ли шифр Вермана подстановочным? Он моно- полиалфавитный? В чем заключается различие между шифром Вермана и одноразовым блокнотом?

22. Почему алгоритм AES считается очень эффективным? Как реализовать умножение в конечном поле F_{2^8} в алгоритме AES?

23. Почему в наборе параметров открытого ключа (e, N) криптосистемы RSA показатель степени e должен быть взаимно простым с

числом ф(N)?

24. Опишите атаки CPA, CCA и CCA2. Чем они отличаются?

25. Почему любой алгоритм шифрования в криптосистемах с открытым ключом (даже учебный) должен быть устойчивым к атаке CPA?

26. Что такое услуги оракула? Необходимы ли атакующему услуги оракула для расшифровки сообщений в криптосистеме с открытым ключом?

27. При каких условиях алгоритм шифрования RSA обладает свойством битовой стойкости?

28. Что обеспечивает стойкость алгоритмов, использующих генератор псевдослучайных чисел Блюма–Блюма–Шаба?

29. Проанализируйте фатальную уязвимость схемы Рабина для активных атак. Почему нестрогая стойкость учебных схем цифровых подписей непригодна для практического применения?

30. Является ли зашифрованный текст, созданный алгоритмом RSA–OAEP, корректным кодом MDC? Если является обоснуйте свой ответ.

31. Перечислите, какие виды угроз информационной безопасности в РФ существуют?

32. Перечислите внешние и внутренние источники угроз? В чем они отличаются?

33. Назовите основные задачи по обеспечению информационной безопасности в РФ?

34. Какие методы обеспечения информационной безопасности РФ существуют? В чем их отличия?

35. Перечислите сферы общественной жизни, которые затрагивают особенности обеспечения информационной безопасности РФ? В чем их особенности?

36. Какие существуют основные направления международного сотрудничества РФ? Чем они отличаются?

37. Назовите основные принципы государственной политики обеспечения информационной безопасности РФ? В чем отличия каждого из них?

38. Назовите первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности РФ? Какие они имеют отличия?

39. Какие основные функции обеспечения информационной безопасности РФ? Их особенности?

40. Основные элементы организационной основы системы обеспечения информационной безопасности РФ? Для чего они предназначены?

41. Какие виды деятельности в структуре правового обеспечения информационной безопасности вы знаете? В чем они отличаются?

42. Назовите составляющие, входящие в состав нормативного правового обеспечения информационной безопасности РФ? Дайте им полное описание?

43. Какие существуют принципы нормативного правового обеспечения информационной безопасности? Дайте им описание?

44. Назовите направления противоправных, злоумышленных действий на сетевой среде с целью использования их результатов для проведения террористических актов? Дайте им объяснения?

45. Назовите набор потенциальных сценариев террористических действий с использованием сетевой среды (Интернет) в самой общей постановке, в качестве взаимодействующих факторов, характеризующих «типовой профиль»? Дайте определения?

46. Назовите меры, которые будут способны противостоять угрозе конфиденциальности? Объясните их?

47. Чем отличается вирус от трояна?

48. Чем отличается SQL – инъекция от php – инклуда?

49. Объясните значение VBR–руткит?

50. Перечислите виды хешей, которые вы знаете (не менее 5)?

Контрольная работа 2

7. Проанализировать содержание понятия разрешительной системы доступа персонала к конфиденциальным сведениям фирмы.

8. Проанализировать состав показателей (граф и зон) перечня конфиденциальных сведений фирмы, обосновать целевое назначение показателей и их взаимосвязь.

9. Регламентировать в виде фрагмента инструкции порядок доступа персонала к
электронным конфиденциальным документам фирмы.

10. Обосновать критерии выделения конфиденциальных документов из общего потока поступающих документов.

Критерии оценки:

- оценка «отлично» выставляется студенту, если верно и правильно выполнено 90%-100% заданий;
- оценка «хорошо» выставляется студенту, если верно и правильно выполнено 70%-80% заданий;
- оценка «удовлетворительно» выставляется студенту, если верно и правильно решено 50%-60% заданий, возможны некоторые исправления при решении;
- оценка «неудовлетворительно» выставляется студенту, если верно выполнено менее 50% заданий;

Вопросы для коллоквиумов, собеседования

Модуль1.

1. Предмет, цели и задачи дисциплины “Информационная безопасность и защита информации”. Основные определения и понятия.

2. Классификация информационных ресурсов, характеристика и основные свойства. Информационные ресурсы в современных условиях, требования к ним, надежность (достоверность) информации и защиты от несанкционированного доступа.
Классификация и анализ угроз информационной безопасности корпоративным системам. Уровни защиты информации: правовой; организационный; аппаратно-программный; криптографический
3. Классификация криптографических методов. Традиционные (симметричные) криптосистемы. Блоковые и поточные шифры. Стойкость криптосистем. Американский стандарт шифрования данных DES. Отечественный стандарт криптографической защиты ГОСТ 28147-89. Асимметричные криптосистемы. Математические основы криптографии с открытым ключом. Криптосистема RSA. Криптосистема Эль Гамаля. Криптосистемы без передачи ключей. Управление ключами. Методы генерации, хранения и распределения ключей. Протоколы управления ключами
4. «Аппаратно-программные решения защиты информации в информационных системах»
План-вопросы
5. Аппаратно-программные средства контроля доступа
5.1. iButton.
5.2 Смарт-карты.
5.3. Устройства ввода на базе USB-ключей.
5.4. Proximity.
5.5. Биометрические УВИП
5.6. Комбинированные устройства ввода.
5.7. Электронные замки
5.8.Инфраструктура открытых ключей. Цифровые сертификаты. Электронная цифровая подпись (ЭЦП). Однонаправленная хэш-функция.

Модуль 2

6. Идентификация и аутентификация объектов сети. Идентификация и подтверждение подлинности пользователей сети.
«Математические методы обеспечения защиты от несанкционирован-ного доступа и конфиденциальности»
План-вопросы
6. Исторический очерк развития криптографии
6.1. Криптография древнего периода
6.2. Криптография арабского мира
6.3. Криптография в эпоху Возрождения (XIV--XVI вв.)
6.4. Криптография в XVII--XVIII веках
6.5. Криптография в XIX веке
6.6. Криптография в XX веке
6.7. О криптографии нового времени
8. Криптография: понятия, подходы, направления исследований
8.1 Предисловие

8.2. Базовая терминология
8.3. Основные алгоритмы шифрования
8.4. Цифровые подписи
8.5. Криптографические хэш-функции
8.6. Криптографические генераторы случайных чисел
8.7. Обеспечиваемая шифром степень защиты
9.8. Криптоанализ и атаки на криптосистемы
9.Межсетевое экранирование. Принципы построения и функционирования межсетевых экранов (МЭ). Классификация МЭ. Особенности межсетевого экранирования на различных уровнях модели OSI
«Криптография и криптоанализ в авторизации, аутентификации и в обмене информации»
План –вопросы
10. Основные понятия и принципы криптографии
10.1 Симметричные криптосистемы
10.2 Асимметричные криптосистемы
10.3 Электронная цифровая подпись
10.4 Управление ключами в криптографических системах защиты информации
11 Особенности реализация криптографических методов
11.1 Федеральная инфраструктура открытых ключей
11.2 Направления исследований в области криптосистем.
12. Средства антивирусной защиты. Классификация вирусов и средств защиты. Виды антивирусных программных продуктов. Характеристика наиболее популярных антивирусных пакетов.
«Информационная безопасность в глобальном информационном пространстве Интернет. Безопасная интеграция в Интернет. Программные и технологические решения»
План-вопросы
13.Угрозы и риски интернет-технологий
14. Стандартизация информационной безопасности в Интернет
4.3 Программно-аппартные технологии Интернет
14.1 Брандмауэры
14.2 Программное обеспечение защиты информации в Интернет
15. Основные понятия и принципы криптографии
15.1 Симметричные криптосистемы
15.2 Асимметричные криптосистемы
15.3 Электронная цифровая подпись
15.4 Управление ключами в криптографических системах защиты информации
16. Особенности реализация криптографических методов

Критерии оценки:

- оценка «отлично» выставляется студенту, если изложение полученных знаний в устной форме полное, в системе, в соответствии с требованиями учебной программы; допускаются единичные

несущественные ошибки, самостоятельно исправляемые учащимися;
- оценка «хорошо» выставляется студенту, если изложение полученных знаний в устной форме полное, в системе, в соответствии с требованиями учебной программы; допускаются, отдельные несущественные ошибки, исправляемые учащимися после указания преподавателя на них;
- оценка «удовлетворительно» выставляется студенту, если изложение полученных знаний неполное, однако это не препятствует усвоению последующего программного материала; допускаются отдельные существенные ошибки, исправляемые с помощью преподавателя;
- оценка «неудовлетворительно» выставляется студенту, если изложение учебного материала неполное, бессистемное, что препятствует усвоению последующей учебной информации; существенные ошибки, не исправляемые даже с помощью преподавателя;

Комплект тестовых заданий для контроля

51 вопрос

Скрыть правильные ответы

1. Вопрос:

Кто является основным ответственным за определение уровня классификации информации?
Варианты ответа:

1. Руководитель среднего звена
2. Высшее руководство
3. Владелец
4. Пользователь

2. Вопрос:

Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
Варианты ответа:

1. Сотрудники
2. Хакеры
3. Атакующие
4. Контрагенты (лица, работающие по договору)

3. Вопрос:

Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

Варианты ответа:

1. Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
2. Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
3. Улучшить контроль за безопасностью этой информации
4. Снизить уровень классификации этой информации

4. Вопрос:

Что самое главное должно продумать руководство при классификации данных?
Варианты ответа:

1. Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
2. Необходимый уровень доступности, целостности и конфиденциальности
3. Оценить уровень риска и отменить контрмеры
4. Управление доступом, которое должно защищать данные
5. Вопрос:

Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?
Варианты ответа:

1. Владельцы данных
2. Пользователи
3. Администраторы
4. Руководство

6. Вопрос:

Что такое процедура?
Варианты ответа:

1. Правила использования программного и аппаратного обеспечения в компании
2. Пошаговая инструкция по выполнению задачи
3. Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах
4. Обязательные действия

7. Вопрос:

Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?
Варианты ответа:

1. Поддержка высшего руководства
2. Эффективные защитные меры и методы их внедрения
3. Актуальные и адекватные политики и процедуры безопасности
4. Проведение тренингов по безопасности для всех сотрудников

8. Вопрос:

Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?
Варианты ответа:

1. Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
2. Когда риски не могут быть приняты во внимание по политическим соображениям
3. Когда необходимые защитные меры слишком сложны
4. Когда стоимость контрмер превышает ценность актива и потенциальные потери

9. Вопрос:

Что такое политики безопасности?
Варианты ответа:

1. Пошаговые инструкции по выполнению задач безопасности
2. Общие руководящие требования по достижению определенного уровня безопасности
3. Широкие, высокоуровневые заявления руководства
4. Детализированные документы по обработке инцидентов безопасности

10. Вопрос:

Какая из приведенных техник является самой важной при выборе конкретных защитных мер?
Варианты ответа:

1. Анализ рисков
2. Анализ затрат / выгоды
3. Результаты ALE
4. Выявление уязвимостей и угроз, являющихся причиной риска

11.Вопрос:

Что лучше всего описывает цель расчета ALE?
Варианты ответа:

1. Количественно оценить уровень безопасности среды
2. Оценить возможные потери для каждой контрмеры
3. Количественно оценить затраты / выгоды
4. Оценить потенциальные потери от угрозы в год

12.Вопрос:

Тактическое планирование – это:
Варианты ответа:

1. Среднесрочное планирование
2. Долгосрочное планирование
3. Ежедневное планирование
4. Планирование на 6 месяцев

13.Вопрос:

Что является определением воздействия (exposure) на безопасность?
Варианты ответа:

1. Нечто, приводящее к ущербу от угрозы
2. Любая потенциальная опасность для информации или систем
3. Любой недостаток или отсутствие информационной безопасности
4. Потенциальные потери от угрозы

14.Вопрос:

Эффективная программа безопасности требует сбалансированного применения:
Варианты ответа:

1. Технических и нетехнических методов
2. Контрмер и защитных механизмов
3. Физической безопасности и технических средств защиты
4. Процедур безопасности и шифрования

15.Вопрос:

Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:
Варианты ответа:

1. Внедрение управления механизмами безопасности

2. Классификацию данных после внедрения механизмов безопасности
3. Уровень доверия, обеспечиваемый механизмом безопасности
4. Соотношение затрат / выгод

16. Вопрос:

Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?
Варианты ответа:

1. Только военные имеют настоящую безопасность
2. Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности
3. Военным требуется больший уровень безопасности, т.к. их риски существенно выше
4. Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности

17. Вопрос:

Как рассчитать остаточный риск?
Варианты ответа:

1. Угрозы х Риски х Ценность актива
2. (Угрозы х Ценность актива х Уязвимости) х Риски
3. SLE х Частоту = ALE
4. (Угрозы х Уязвимости х Ценность актива) х Недостаток контроля

18. Вопрос:

Что из перечисленного не является целью проведения анализа рисков?
Варианты ответа:

1. Делегирование полномочий
2. Количественная оценка воздействия потенциальных угроз
3. Выявление рисков
4. Определение баланса между воздействием риска и стоимостью необходимых контрмер

19. Вопрос:

Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?
Варианты ответа:

1. Поддержка

2. Выполнение анализа рисков
3. Определение цели и границ
4. Делегирование полномочий

20. Вопрос:

Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?
Варианты ответа:

1. Чтобы убедиться, что проводится справедливая оценка
2. Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ
3. Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа
4. Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку

21. Вопрос:

Что является наилучшим описанием количественного анализа рисков?
Варианты ответа:

1. Анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности
2. Метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков
3. Метод, сопоставляющий денежное значение с каждым компонентом оценки рисков
4. Метод, основанный на суждениях и интуиции

22. Вопрос:

Почему количественный анализ рисков в чистом виде не достижим?
Варианты ответа:

1. Он достижим и используется
2. Он присваивает уровни критичности. Их сложно перевести в денежный вид.
3. Это связано с точностью количественных элементов
4. Количественные измерения должны применяться к качественным элементам

23. Вопрос:

Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется так много времени для проведения анализа?
Варианты ответа:

1. Много информации нужно собрать и ввести в программу
2. Руководство должно одобрить создание группы
3. Анализ рисков не может быть автоматизирован, что связано с самой природой оценки
4. Множество людей должно одобрить данные

24. Вопрос:

Какой из следующих законодательных терминов относится к компании или человеку, выполняющему необходимые действия, и используется для определения обязательств?
Варианты ответа:

1. Стандарты
2. Должный процесс (Due process)
3. Должная забота (Due care)
4. Снижение обязательств

25. Вопрос:

Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?
Варианты ответа:

1. Список стандартов, процедур и политик для разработки программы безопасности
2. Текущая версия ISO 17799
3. Структура, которая была разработана для снижения внутреннего мошенничества в компаниях
4. Открытый стандарт, определяющий цели контроля

26. Вопрос:

Из каких четырех доменов состоит CobiT?
Варианты ответа:

1. Планирование и Организация, Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
2. Планирование и Организация, Поддержка и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

3. Планирование и Организация, Приобретение и Внедрение, Сопровождение и Покупка, Мониторинг и Оценка
4. Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

27. Вопрос:

Что представляет собой стандарт ISO/IEC 27799?
Варианты ответа:

1. Стандарт по защите персональных данных о здоровье
2. Новая версия BS 17799
3. Определения для новой серии ISO 27000
4. Новая версия NIST 800-60

28. Вопрос:

CobiT был разработан на основе структуры COSO. Что является основными целями и задачами COSO?
Варианты ответа:

1. COSO – это подход к управлению рисками, который относится к контрольным объектам и бизнес-процессам
2. COSO относится к стратегическому уровню, тогда как CobiT больше направлен на операционный уровень
3. COSO учитывает корпоративную культуру и разработку политик
4. COSO – это система отказоустойчивости

29. Вопрос:

OCTAVE, NIST 800-30 и AS/NZS 4360 являются различными подходами к реализации управления рисками в компаниях. В чем заключаются различия между этими методами?
Варианты ответа:

1. NIST и OCTAVE являются корпоративными
2. NIST и OCTAVE ориентирован на ИТ
3. AS/NZS ориентирован на ИТ
4. NIST и AS/NZS являются корпоративными

30. Вопрос:

Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой?
Варианты ответа:

1. Анализ связующего дерева
2. AS/NZS
3. NIST
4. Анализ сбоев и дефектов

31. Вопрос:

Что было разработано, чтобы помочь странам и их правительствам построить законодательство по защите персональных данных похожим образом?
Варианты ответа:

1. Безопасная OECD
2. ISO\IEC
3. OECD
4. CPTED

32. Вопрос:

Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста, это метод:
Варианты ответа:

1. гаммирования;
2. подстановки;
3. кодирования;
4. перестановки;
5. аналитических преобразований.
6. Символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов, это метод:
7. гаммирования;

33. Вопрос:

подстановки;
Варианты ответа:

1. кодирования;
2. перестановки;
3. аналитических преобразований.

34. Вопрос:

Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, это метод:
Варианты ответа:

1. гаммирования;
2. подстановки;
3. кодирования;
4. перестановки;
5. аналитических преобразований.

35. Вопрос:
Защита информации от утечки это деятельность по предотвращению:
Варианты ответа:

1. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
2. воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
3. воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
4. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
5. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

36. Вопрос:
Защита информации это:
Варианты ответа:

1. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
3. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;

5. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

37.Вопрос:
Естественные угрозы безопасности информации вызваны:
Варианты ответа:

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

38.Вопрос:
38 Икусственные угрозы безопасности информации вызваны:
Варианты ответа:

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

39. Вопрос:
К основным непреднамеренным искусственным угрозам АСОИ относится:
Варианты ответа:

1. физическое разрушение системы путем взрыва, поджога и т.п.;
2. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
4. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
5. неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы.

40.Вопрос:

К посторонним лицам нарушителям информационной безопасности относится:
Варианты ответа:

1. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
2. персонал, обслуживающий технические средства;
3. технический персонал, обслуживающий здание;
4. пользователи;
5. сотрудники службы безопасности.
6. представители конкурирующих организаций.
7. лица, нарушившие пропускной режим;

41.Вопрос:

Спам, который имеет цель опорочить ту или иную фирму, компанию, политического кандидата и т.п:
Варианты ответа:

1. черный пиар;
2. фишинг;
3. нигерийские письма;
4. источник слухов;
5. пустые письма.

42.Вопрос:

Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:
Варианты ответа:

1. черный пиар;
2. фишинг;
3. нигерийские письма;
4. источник слухов;
5. пустые письма.

43.Вопрос:

Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы:
Варианты ответа:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

44.Вопрос:

Антивирус не только находит зараженные вирусами файлы, но и "лечит" их, т.е. удаляет из файла тело программы вируса, возвращая файлы в исходное состояние:
Варианты ответа:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

45.Вопрос:

Антивирус запоминает исходное состояние программ, каталогов и системных областей диска когда компьютер не заражен вирусом, а затем периодически или по команде пользователя сравнивает текущее состояние с исходным:
Варианты ответа:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

46.Вопрос:

. Антивирус представляет собой небольшую резидентную программу, предназначенную для обнаружения подозрительных действий при работе компьютера, характерных для вирусов:
Варианты ответа:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

47.Вопрос:

Активный перехват информации это перехват, который:
Варианты ответа:

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.

48.Вопрос:

Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:
Варианты ответа:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

49.Вопрос:

Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется:
Варианты ответа:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. 5.просмотр мусора.

50.Вопрос:

Перехват, который осуществляется путем использования оптической техники называется:
Варианты ответа:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

51.Вопрос:
К внутренним нарушителям информационной безопасности относится:
Варианты ответа:

1. клиенты;
2. пользователи системы;
3. посетители;
4. любые лица, находящиеся внутри контролируемой территории;
5. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации.
6. персонал, обслуживающий технические средства.
7. сотрудники отделов разработки и сопровождения ПО;
8. технический персонал, обслуживающий здание

Таблица №2.Ответы тестов.

№ Т	№ О	№О	№ Т	№О	№О	№ Т	№О	№О
1	в	3	18	а	1	35	г	4
2	а	1	19	б	2	36	д	2
3	в	3	20	в	3	37	в	3
4	б	2	21	в	2	38	а	1
5	г	4	22	г	4	39	д	5
6	б	2	23	а	1	40	е	6
7	а	1	24	в	3	41	а	1
8	г	4	25	г	4	42	б	2
9	в	3	26	а	1	43	а	1
10	б	2	27	а	1	44	б	2
11	г	4	28	б	2	45	г	4
12	а	1	29	б	2	46	д	5
13	а	1	30	г	4	47	д	5
14	а	1	31	в	3	48	в	3
15	в	3	32	Г,е	4.6	49	б	2
16	б	2	33			50	г	4
17	г	4	34	а	1	51	з	8

Критерии оценки:

- оценка «отлично» выставляется студенту, если верно и правильно выполнено 90%-100% заданий;
- оценка «хорошо» выставляется студенту, если верно и правильно выполнено 70%-80% заданий;
- оценка «удовлетворительно» выставляется студенту, если верно и правильно решено 50%-60% заданий, возможны некоторые исправления при решении;
- оценка «неудовлетворительно» выставляется студенту, если верно выполнено менее 50% заданий;

Темы эссе (рефератов, докладов, сообщений)

1. Номер варианта контрольной работы определяется по последней цифре номера зачетной книжки (или по последней цифре порядкового номера Ф.И.О. студента в списке журнала группы, если он взят за основу при определении варианта); цифра «10» означает вариант № 10. Распределение теоретических вопросов по вариантам приведено в таблице1.

Таблица №3 – Распределение теоретических вопросов по вариантам

№ варианта	Номера вопросов				
1	1	11	21	31	41
2	2	12	22	32	42
3	3	13	23	33	43
4	4	14	24	34	44
5	5	15	25	35	45
6	6	16	26	36	46
7	7	17	27	37	47
8	8	18	28	38	48
9	9	19	29	39	49
10	10	20	30	40	50

2. Работа должна быть оформлена с помощью любого текстового процессора. . К текстам, подготовленным с помощью текстового процессора, предъявляются следующие требования: шрифт

a. Times New Roman, 14;
b. междустрочный интервал 1,5;
c. поля: верхнее – 2см, нижнее – 2 см, левое – 2,5 см, правое – 1,5 см;
d. выравнивание абзацев по ширине;
e. абзацный отступ 1,25 см;

f. выравнивание заголовков по ширине,
g. шрифт для заголовков 1 уровня Times New Roman, 16 пт, полужирный;
h. для заголовков 2 уровня и далее - Times New Roman, 14 пт, полужирный;
i. нумерация страниц – внизу страницы, посередине;
j. обязательно наличие автооглавления;

52. В конце работы необходимо указать список использованных источников.
53. Практическое задание №1 (презентация) и практическое задание № 2 (файл с программой) должны быть представлены на любом электронном носителе.
54. В начале работы должен быть указан номер варианта задания.
55. На лицевой стороне контрольной работы необходимо указать следующую информацию: Ф.И.О. студента, номер группы, дисциплина и номер зачетной книжки (или, соответственно, порядковый номер Ф.И.О. студента в списке журнала группы).

Теоретические вопросы

1. Что такое информационная безопасность? Какие компоненты входят в информационную безопасность? Назовите пять этапов процесса информационной безопасности.
2. Почему безопасность – это процесс, а не конечный продукт?
3. Почему физическая защита не может гарантировать безопасность?
4. Выделите два основных типа межсетевых экранов. От какого нападения защищают межсетевые экраны?
5. Назовите основные категории атак. Всегда ли атака модификации включает в себя атаку доступа?
6. Назовите основные категории атак. К какому типу атак особенно уязвимы беспроводные сети?
7. Что определяет политика безопасности? Почему в политику безопасности включают отказы от защиты?
8. Угрозы и их составляющие. Может ли угроза иметь более одной цели? Назовите четыре цели для угроз.
9. Что определяет политика безопасности? Назовите четыре необходимых политики безопасности.
10. Назовите основные категории атак. Каковы три вида атак на схему шифрования?
11. Назовите три типа аутентификационных факторов. Почему двухфакторная аутентификация сильнее, чем однофакторная?
12. Зачем нужен аудит? На какие три службы безопасности должен опираться аудит?
13. Что такое уязвимость? Основные виды уязвимостей и их отличия. Приведите несколько рекомендаций по устранению уязвимостей.
14. Назовите две составляющих риска. Каков уровень риска при

отсутствии угроз?

15. Назовите ключевые концепции стандарта ISO, в котором говорится об информационной безопасности.

16. Может ли шифрование полностью защитить данные, передаваемые через VPN.

17. Какие механизмы аутентификации лучше всего использовать для пользовательской VPN?

18. Что подразумевается под пассивными ответными действиями? Что подразумевается под активными ответными действиями?

19. Каков приблизительный радиус действия беспроводной сети стандарта 802.11x на открытой местности и в помещении? Почему аутентификация 802.1X сама по себе рассматривается как уязвимость в системе?

20. К какому типу сетей следует относить WLAN? Какую периодическую оценку необходимо проводить при работе с WLAN?

21. Является ли шифр Вермана подстановочным? Он моно-полиалфавитный? В чем заключается различие между шифром Вермана и одноразовым блокнотом?

22. Почему алгоритм AES считается очень эффективным? Как реализовать умножение в конечном поле F_{2^8} в алгоритме AES?

23. Почему в наборе параметров открытого ключа (e, N) криптосистемы RSA показатель степени e должен быть взаимно простым с числом ф(N)?

24. Опишите атаки CPA, CCA и CCA2. Чем они отличаются?

25. Почему любой алгоритм шифрования в криптосистемах с открытым ключом (даже учебный) должен быть устойчивым к атаке CPA?

26. Что такое услуги оракула? Необходимы ли атакующему услуги оракула для расшифровки сообщений в криптосистеме с открытым ключом?

27. При каких условиях алгоритм шифрования RSA обладает свойством битовой стойкости?

28. Что обеспечивает стойкость алгоритмов, использующих генератор псевдослучайных чисел Блюма–Блюма–Шаба?

29. Проанализируйте фатальную уязвимость схемы Рабина для активных атак. Почему нестрогая стойкость учебных схем цифровых подписей непригодна для практического применения?

30. Является ли зашифрованный текст, созданный алгоритмом RSA–OAEP, корректным кодом MDC? Если является обоснуйте свой ответ.

31. Перечислите, какие виды угроз информационной безопасности в РФ существуют?

32. Перечислите внешние и внутренние источники угроз? В чем они отличаются?

33. Назовите основные задачи по обеспечению информационной безопасности в РФ?

34. Какие методы обеспечения информационной безопасности РФ существуют? В чем их отличия?

35. Перечислите сферы общественной жизни, которые затрагивают особенности обеспечения информационной безопасности РФ? В чем их особенности?

36. Какие существуют основные направления международного сотрудничества РФ? Чем они отличаются?

37. Назовите основные принципы государственной политики обеспечения информационной безопасности РФ? В чем отличия каждого из них?

38. Назовите первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности РФ? Какие они имеют отличия?

39. Какие основные функции обеспечения информационной безопасности РФ? Их особенности?

40. Основные элементы организационной основы системы обеспечения информационной безопасности РФ? Для чего они предназначены?

41. Какие виды деятельности в структуре правового обеспечения информационной безопасности вы знаете? В чем они отличаются?

42. Назовите составляющие, входящие в состав нормативного правового обеспечения информационной безопасности РФ? Дайте им полное описание?

43. Какие существуют принципы нормативного правового обеспечения информационной безопасности? Дайте им описание?

44. Назовите направления противоправных, злоумышленных действий на сетевой среде с целью использования их результатов для проведения террористических актов? Дайте им объяснения?

45. Назовите набор потенциальных сценариев террористических действий с использованием сетевой среды (Интернет) в самой общей постановке, в качестве взаимодействующих факторов, характеризующих «типовой профиль»? Дайте определения?

46. Назовите меры, которые будут способны противостоять угрозе конфиденциальности? Объясните их?

47. Чем отличается вирус от трояна?

48. Чем отличается SQL – инъекция от php – инклуда?

49. Объясните значение VBR–руткит?

50. Перечислите виды хешей, которые вы знаете (не менее 5)?

Реферат оценивается следующим образом:

- соответствие содержания теме- 4 балла;
- глубина проработки материала, 3 балла;
- грамотность и полнота использования источников, 1 балл;
- соответствие оформления реферата требованиям, 2 балла;
- доклад, 5 баллов;

- умение вести дискуссию и ответы на вопросы, 5 баллов.

Максимальное количество баллов: 20.

Критерии оценки:

- оценка «отлично» выставляется студенту, если набрал 19-20 баллов;
- оценка «хорошо» выставляется студенту, если набрал 15-18 баллов;
- оценка «удовлетворительно» выставляется студенту, если набрал 10-14 баллов;
- оценка «неудовлетворительно» выставляется студенту, если набрал менее 10 баллов;

Вопросы к экзамену

1. Предмет, цели и задачи дисциплины .
2. Основные определения и понятия.
3. Законодательство в области информационной безопасности и защиты данных.
4. Структуры и нормативные акты, их направления»
5. Классификация нормативных актов в области ИБ и ЗД:
6. Государственные органы, регулирующие вопросы информационной безопасности
7. Классификация информации по степени ее защиты
8. Доктрина информационной безопасности РФ
9. Законодательство и нормативные акты Российской Федерации.
10. Классификация информационных ресурсов, характеристика и основные свойства.
11. Информационные ресурсы в современных условиях, требования к ним, надежность (достоверность) информации и защиты от несанкционированного доступа.
12. Классификация и анализ угроз информационной безопасности корпоративным системам.
13. Уровни защиты информации: правовой; организационный; аппаратно-программный; криптографический
14. Классификация криптографических методов.
15. Традиционные (симметричные) криптосистемы.
16. Блоковые и поточные шифры.
17. Стойкость криптосистем.
18. Американский стандарт шифрования данных DES.
19. Отечественный стандарт криптографической защиты ГОСТ 28147-89.
20. Асимметричные криптосистемы.
21. Математические основы криптографии с открытым ключом.
22. Криптосистема RSA.
23. Криптосистема Эль Гамаля.
24. Криптосистемы без передачи ключей.
25. Управление ключами.
26. Методы генерации, хранения и распределения ключей.
27. Протоколы управления ключами

28. Аппаратно-программные решения защиты информации в информационных системах.
29. Аппаратно-программные средства контроля доступа
30.. iButton.
31. Смарт-карты.
32. Устройства ввода на базе USB-ключей.
33. Proximity.
34. Биометрические УВИП
35. Комбинированные устройства ввода.
36. Электронные замки
37. Инфраструктура открытых ключей.
38. Цифровые сертификаты.
39. Электронная цифровая подпись (ЭЦП).
40. Однонаправленная хэш-функция.
41. Идентификация и аутентификация объектов сети.
42. Идентификация и подтверждение подлинности пользователей сети.
43. Математические методы обеспечения защиты от несанкционированного доступа и конфиденциальности»
44. Исторический очерк развития криптографии
45. Криптография древнего периода
46. Криптография арабского мира
47. Криптография в эпоху Возрождения (XIV--XVI вв.)
48. Криптография в XVII--XVIII веках
49. Криптография в XIX веке
50. Криптография в XX веке
51. О криптографии нового времени
52.. Криптография: понятия, подходы, направления исследований
53.. Базовая терминология
54. Основные алгоритмы шифрования
55. Цифровые подписи
56. Криптографические хэш-функции
57. Криптографические генераторы случайных чисел
58. Обеспечиваемая шифром степень защиты
59. Криптоанализ и атаки на криптосистемы
60.. Межсетевое экранирование.
61. Принципы построения и функционирования межсетевых экранов (МЭ). Классификация МЭ.
62. Особенности межсетевого экранирования на различных уровнях модели OSI
63. Криптография и криптоанализ в авторизации, аутентификации и в обмене информации.
64. Основные понятия и принципы криптографии
65. Симметричные криптосистемы
66. Асимметричные криптосистемы
67. Электронная цифровая подпись

68. Управление ключами в криптографических системах защиты информации
69. Особенности реализация криптографических методов
70. Федеральная инфраструктура открытых ключей
71. Направления исследований в области криптосистем.
72. Средства антивирусной защиты.
73. Классификация вирусов и средств защиты.
74. Виды антивирусных программных продуктов.
75. Характеристика наиболее популярных антивирусных пакетов.
76. Архитектура системы защиты информации (СЗИ).
77. Этапы создания СЗИ. Виды обеспечения СЗИ.
78. Принципы разработки СЗИ.
79. «Информационная безопасность в глобальном информационном пространстве Интернет.
80. Безопасная интеграция в Интернет.
81. Программные и технологические решения»
82. Угрозы и риски интернет-технологий
83. Стандартизация информационной безопасности в Интернет
84. Программно-аппартные технологии Интернет
85. Брандмауэры
86. Программное обеспечение защиты информации в Интернет
87. Основные понятия и принципы криптографии
88. Симметричные криптосистемы
89. Асимметричные криптосистемы
90. Электронная цифровая подпись
91. Управление ключами в криптографических системах защиты информации
92. Особенности реализация криптографических методов
93. Серверы доступа (брандмауэры) Cisco ASA5500.
94. Средства обнаружения вторжений IDS 4200.

Критерии оценки:

- оценка «отлично» выставляется студенту, если изложение полученных знаний в устной форме полное, в системе, в соответствии с требованиями учебной программы; допускаются единичные несущественные ошибки, самостоятельно исправляемые учащимися;
- оценка «хорошо» выставляется студенту, если изложение полученных знаний в устной форме полное, в системе, в соответствии с требованиями учебной программы; допускаются, отдельные несущественные ошибки, исправляемые учащимися после указания преподавателя на них;
- оценка «удовлетворительно» выставляется студенту, если изложение полученных знаний неполное, однако это не препятствует усвоению последующего программного материала; допускаются отдельные существенные ошибки, исправляемые с помощью преподавателя;

- оценка «неудовлетворительно» выставляется студенту, если изложение учебного материала неполное, бессистемное, что препятствует усвоению последующей учебной информации; существенные ошибки, не исправляемые даже с помощью преподавателя;

Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

1. . а) адрес сайта курса
2. Интернет-адрес сайта. eLIBRARY.RU[Электронный ресурс]: электронная библиотека / Науч. электрон. б-ка. — Москва, 1999 – Режим доступа: http://elibrary.ru/defaultx.asp– Яз. рус., англ.
3. Электронный каталог НБ ДГУ[Электронный ресурс]: база данных содержит сведения о всех видах лит, поступающих в фонд НБ ДГУ/Дагестанский гос. ун-т. – Махачкала, 2010 – Режим доступа: http://elib.dgu.ru, свободный .
4. Список основной литературы

5. Галатенко, Владимир Антонович.и Основы информационной безопасности : учеб. пособие для студентов вузов, обуч. по специальности 351400 "Прикл. информ." / Галатенко, Владимир Антонович. - 4-е изд. - М. : Изд-во Интернет-Ун-та Информ. Технологий: БИНОМ. Лаб. знаний, 2016, 2008, 2006. - 205 с. - (Основы информационных технологий). - Рекомендовано УМО. - ISBN 978-5-94774-821-5 : 230-00.Местонахождение: Университетская библиотека ONLINE, IPRbooks URL:http://biblioclub.ru/index.php?page=book&id=233063, http://www.iprbookshop.ru/52209.html

6. Мельников, Владимир Павлович. Информационная безопасность и защита информации : учеб. пособие для студентов вузов, обуч. по специальности "Информ. системы и технологии" / Мельников, Владимир Павлович, С. А. Клейменов ; под ред. С.А.Клейменова. - 5-е изд., стер. - М. : Академия, 2011, 2010. - 330,[6] с. - (Высшее профессиональное образование. Информатика и вычислительная техника). - Допущено УМО. - ISBN 978-5-7695-7738-3 : 401-06. Местонахождение: Научная библиотека ДГУ (Дата обращения 10.12.2017 г.)

7. Бабаш, Александр Владимирович. Информационная безопасность : лаб. практикум; учеб. пособие / Бабаш, Александр Владимирович, Е. К. Баранов. - 2-е изд., стер. - И. : Кнорус, 2016, 2011. - 306-00.
Местонахождение: Университетская библиотека ONLINE URL: http://biblioclub.ru/index.php?page=book&id=90539

8. Сергеева, Ю.С. Защита информации. : Конспект лекций. Учебное пособие / Ю. С. Сергеева ; Сергеева Ю. С. - М. : А-Приор, 2011. - 128. - (Конспект лекций). - ISBN 978-5-384-00397-7.

Местонахождение: Российская государственная библиотека (РГБ) URL: http://нэб.рф/catalog/000199_000009_006559182/

9. Прохорова, О.В. Информационнаябезопасность и защитаинформации : учебник / О.В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». - Самара : Самарский государственный архитектурно-строительный университет, 2014. - 113 с. : табл., схем., ил. - Библиогр. в кн. - ISBN 978-5-9585-0603-3 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=438331

10. Инструментальный контроль и защитаинформации : учебное пособие / Н.А. Свинарев, О.В. Ланкин, А.П. Данилкин и др. ; Министерство образования и науки РФ, ФГБОУ ВПО «Воронежский государственный университет инженерных технологий». - Воронеж : Воронежский государственный университет инженерных технологий, 2013. - 192 с. : табл., ил. - Библиогр. в кн. - ISBN 978-5-00032-018-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=255905

11. Бурькова, Е.В. Физическая защита объектов информатизации : учебное пособие / Е.В. Бурькова ; Министерство образования и науки Российской Федерации, Оренбургский Государственный Университет, Кафедра вычислительной техники и защиты информации. - Оренбург : Оренбургский государственный университет, 2017. - 158 с. : табл., схем. - Библиогр. в кн. - ISBN 978-5-7410-1697-8 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=481730

Дпольнительная

1. Алешников С.И. Математические методы защиты информации. Часть 4. Вычислительный практикум по эллиптическим кривым и криптографии на эллиптических кривых [Электронный ресурс] : практическое пособие / С.И. Алешников, Ю.Ф. Болтнев. — Электрон. текстовые данные. — Калининград: Балтийский федеральный университет им. Иммануила Канта, 2007. — 58 с. — 978-588874-803-9. — Режим доступа: http://www.iprbookshop.ru/23795.html

2. Алешников С.И. Математические методы защиты информации. Часть 5. Методы алгебраических кривых [Электронный ресурс] : учебное пособие / С.И. Алешников, Е.С. Алексеенко. — Электрон. текстовые данные. — Калининград: Балтийский федеральный университет им. Иммануила Канта, 2010. — 158 с. — 9785-9971-0073-5. — Режим доступа: http://www.iprbookshop.ru/23796.html

3. Алешников С.И. Математические методы защиты информации. Часть 3. Вычислительный практикум по числовым полям и криптографии в квадратичных полях [Электронный ресурс] : практическое пособие / С.И.

Алешников, Е.В. Козьминых. — Электрон. текстовые данные. — Калининград: Балтийский федеральный университет им. Иммануила Канта, 2006. — 97 с. — 588874-689-4. — Режим доступа: http://www.iprbookshop.ru/23851.html

4. Бескид П.П. Криптографические методы защиты информации. Часть 2. Алгоритмы, методы и средства обеспечения конфиденциальности, подлинности и целостности информации [Электронный ресурс] : учебное пособие / П.П. Бескид, Т.М. Тагарникова. — Электрон. текстовые данные. — СПб. : Российский государственный гидрометеорологический университет, 2010. — 104 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/17926.html

Интернет-ресурсы:

1. Википедия – свободная энциклопедия [Электронный ресурс] – Режим доступа:http://ru.wikipedia.org – ;
2. ИНТУИТ. Национальный открытый университет. Проект Издательства «Открытые Системы». [Электронный ресурс] – Режим доступа: http://Intuit.ru
3. Научная электронная библиотека; [Электронный ресурс] – Режим доступа: www.elibrary.ru –
4. Новая электронная библиотека [Электронный ресурс] – Режим доступа: www.newlibrary.ru -;
5. Общероссийский математический портал [Электронный ресурс] – Режим доступа: www.mathnet.ru –;
6. Федеральный портал российского образования [Электронный ресурс] – Режим доступа: www.edu.ru –;
7. Электронная библиотека учебных материалов [Электронный ресурс] – Режим доступа: www.nehudlit.ru –.