ПРОГРАММА
вступительного испытания в магистратуру по направлению 10.04.01 - Информационная безопасность

1. Основные теории экономической стратегии фирмы. Структура управления фирмой и факторы ее определяющие.
2. Основные ценовые стратегии: стратегия дифференцированного ценообразования, стратегия конкурентного ценообразования, стратегия ассортиментного ценообразования.
3. Анализ финансового состояния фирмы и его использование в управленческой деятельности.
4. Управление рисками в механизме обеспечения экономической безопасности фирмы.
5. Пуассоновский случайный процесс, его среднее значение и корреляционная функция.
6. Конечные однородные цепи Маркова. Переходные вероятности. Простейшая классификация состояний конечной цепи Маркова.
7. Винеровский случайный процесс. Броуновское движение.
8. Демаскирующие признаки объектов защиты. Демаскирующие признаки объектов в видимом и ИК-диапазоне электромагнитного спектра. Демаскирующие признаки аналоговых и цифровых сигналов радиоэлектронных средств.
9. Физическая природа побочных электромагнитных излучений и наводок (ПЭМИН). Основные уравнения электромагнитного поля. Виды ПЭМИН. ПЭМИН персонального компьютера (ПК). Способы предотвращения утечки информации через ПЭМИН ПК.
10. Физические основы возникновения акустического (виброакустического) канала утечки информации. Структура, классификация и основные характеристики акустических каналов утечки информации. Понятность и разборчивость речи. Средства акустической разведки.
11. Скрытие речевой информации в телефонных системах связи с использованием технического закрытия речевых сигналов. Классификация методов технического закрытия. Аналоговые скремблеры: состав, принцип работы, технические характеристики. Системы цифрового закрытия речи: состав, принцип работы, технические характеристики. Вокодеры: назначение, классификация, принцип работы.
12. Криптография на основе эллиптических кривых. Суть применения эллиптических кривых в криптографии.

13. Современные криптографические алгоритмы симметричной криптографии: ГОСТ 28147-89, AES. Архитектура, режимы использования.
14. Однонаправленные хеш-функции. Хеш-функции с ключом. Современные алгоритмы. Построение хеш-функции с использованием алгоритма шифрования.
15. Расстояние единственности. Понятие, возможности криптоанализа. Криптографические протоколы. Протокол Kerberos. Стандарт X.509
16. Инфраструктура открытых ключей (PKI) и удостоверяющие центры в корпоративных системах. Области применения криптографических методов. Построение VPN на PKI.
17. Каково основное назначение межсетевых экранов? Типы межсетевых экранов. Какие действия осуществляются межсетевым экраном в отношении трафика? Почему порядок правил в наборе правил межсетевого экрана играет важную роль? Преимущества и недостатки межсетевых экранов.
18. Перечислите основные устройства межсетевого взаимодействия. Перечислите основные составляющие эшелонированной обороны. Сформулируйте определение демилитаризованной зоны. Что такое сетевой периметр? Перечислите основные механизмы и службы защиты.
19. Безопасность сетевого оборудования. Принцип работы коммутатора и маршрутизатора. Методы обеспечения безопасности коммутаторов. Списки контроля доступа.
20. Дать понятие атаки на компьютерную систему. Перечислите основные угрозы при сетевом взаимодействии. Что понимается под удаленной сетевой атакой? Виды атак и их характеристика. В чём сходства и отличия понятий угрозы и уязвимости. Виды уязвимостей вычислительных сетей и их характеристика («buffer overflow», «SQL Injection», «format string», «Directory traversal», «Cross Site Scripting» и уязвимости программных реализаций стека TCP/IP).
21. Классификации удаленных атак. Списки категорий. Матричные схемы. Перечислите основные средства атак по классификации Ховарда. Перечислите основные различия онтологии и таксономии. Что понимается под эксплойтом? Какая взаимосвязь между атакой и сценарием атаки? Перечислите основные шаги обобщенного сценария атаки. Каково главное отличие атаки от вторжения? Что может быть установлено на атакуемой системе в результате успешной атаки? Оценивание степени серьезности атак.
22. Сущность аутентификации при удалённом доступе. Идентификация и аутентификация пользователей. Однофакторная и многофакторная аутентификация. Алгоритм, достоинства и недостатки аутентификации пользователей на основе модели «рукопожатия» («запрос-ответ»). Способы

повышения безопасности протокола взаимной аутентификации. Алгоритм аутентификации на основе паролей. Какие виды атак на пароль Вы знаете? Параметры политики учётных записей при использовании парольной аутентификации и способы их реализации. Алгоритм, достоинства и недостатки аутентификации пользователей на основе протокола Kerberos. Для чего предназначен протокол Kerberos?
23. Виды трансляции адресов. Каково значение функции трансляции адресов с точки зрения обеспечения информационной безопасности? Чем отличается NAT от PAT? Принципы образования сетевых адресов. Настройка общего доступа в Интернет. Настройка NAT с помощью маршрутизации и удалённого доступа.
24. В чём заключается сущность систем обнаружения (предупреждения) атак? Почему следует использовать систем обнаружения атак? Типы системы обнаружения атак и вторжений. Выбор систем обнаружения атак. Размещение систем обнаружения атак. Системы типа «honeypot». Последствия - конечный результат атаки.
25. В чём состоят функции средств анализа защищённости компьютерных систем и каковы их основные достоинства и недостатки? Чего не делает сканирование уязвимостей? Настройка и конфигурирование сканирования уязвимостей. Подготовка отчетов. Особенности сканирования уязвимостей.
26. Виды защищённого подключения к удалённым сетям. Безопасность виртуальных частных сетей. Как работает VPN. Протоколы VPN. Режимы работы VPN.
27. Безопасность беспроводных сетей. Недостатки шифрования. Методы и рекомендации по повышению беспроводной сети. Основные принципы обнаружения вторжений в беспроводных сетях.
28. Задача идентификации пользователя. Понятие протокола идентификации. Локальная и удаленная идентификация. Идентифицирующая информация. Способы хранения идентифицирующей информации. Связь с ключевыми системами.
29. Модели разграничения доступа. Дискреционная модель. Мандатная модель. Реализация в ОС и средствах защиты информации.
30. Концепция защиты информации от НСД. Руководящие документы ФСТЭК по оценке защищенности от НСД. Государственные требования к построению СЗИ.
31. Подсистемы защиты современных операционных систем. Субъекты, объекты, методы и права доступа в современных операционных системах. Основные компоненты подсистем защиты UNIX и Windows.

32. Защита информации в вычислительных сетях и базах данных. Программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях;
33. Типовые решения в организации ключевых систем. Распределение ключей симметричного шифрования. Алгоритм DH.
34. Открытое распределение ключей. Распределение ключей асимметричного шифрования и ЭЦП. Ключевая система и ключевые носители СКЗИ «КриптоПро». Управление ключами СКЗИ «КриптоПро».
35. Механизм заражения программ вирусами. Необходимые и достаточные условия недопущения разрушающего воздействия. Понятие изолированной программной среды

ОСНОВНАЯ ЛИТЕРАТУРА

1. Курс экономической теории. Под ред. Чепурина М.Н., Киселевой Е.А. 5-е изд. , испр., дополн. и перераб. - Киров: "АСА", 2006. — 832 с.
2. Глухов М.М., Круглов И.А., Пичкур А.Б., Черемушкин А.В. Введение в теоретико-числовые методы криптографии. СПб: Лань, 2011. – 400 с.
3. Соболев А.Н., Кириллов В.М. Физические основы технических средств обеспечения информационной безопасности: Учебное пособие: Рекомендовано УМО вузов по образованию в области информационной безопасности в качестве учебного пособия для студентов высших учебн. заведений. М.: Гелиос АРВ, 2011. 224 с.
4. Смирнов С.Н. Безопасность систем баз данных. Учебное пособие для вузов. М.: Гелиос-АРВ, 2007. – 351 с.: ил.
5. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информации: учеб. пособие для студентов вузов. Под ред. Зайцева А.П. и Шелупанова А.А.. Изд. 4-е испр. и доп. − М.: Горячая линия-Телеком, 2009.
6. Серия «Вопросы управление информационной безопасностью». Часть 1: Основы управления информационной безопасностью Учебное пособие. для вузов / А.П. Курило, Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2012. – 206 с.
7. Серия «Вопросы управления информационной безопасностью». Часть 2: Управление рисками информационной безопасности: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2012. – 113 с.
8. Хорев П.В. Программно-аппаратная защита информации: учебное пособие / П.Б. Хорев. – М.: ФОРУМ, 2009 - 352 с. Ил.

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

1. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО, 2007 – 328 с.
2. Холево А.С. Квантовые системы, каналы, информация. М.: МЦНМО, 2010. 328 с.
3. Петренко С., Симонов С. Управление информационными рисками. Экономически оправданная безопасность. — М.: АйТи-Пресс, 2004. — 392 с.
4. Галатенко В.А. Стандарты информационной безопасности. Курс лекций. – М.: Издательство: Интернет-университет информационных технологий, 2004. – 328 с.
5. Обеспечение информационной безопасности деятельности учебного заведения / В.А. Шевцов, В.П. Мельников, А.И. Куприянов, А.М. Петраков; под ред. проф. В.П. Мельникова.- М.: Вузовская книга, 2012.