ПРОГРАММА

вступительного испытания в магистратуру

по направлению 10.04.01 - Информационная безопасность

1. Управление рисками в механизме обеспечения информационной безопасности организации.
2. Формирование затрат на обеспечение информационной безопасности и непрерывности бизнеса.
3. Методика формирования цены на информационные продукты и услуги.
4. Методика расчета экономического эффекта и эффективности обеспечения информационной безопасности.
5. Расчёт экономического эффекта и экономической эффективности обеспечения безопасности АС.
6. Основные экономические показатели функционирования автоматизированных систем.
7. Основные положения экономической эффективности обеспечения безопасности автоматизированных систем.
8. Технико-экономическое обоснование разработки проекта системы обеспечения информационной безопасности.
9. Пуассоновский случайный процесс, его среднее значение и корреляционная функция.
10. Конечные однородные цепи Маркова. Переходные вероятности. Простейшая классификация состояний конечной цепи Маркова.
11. Винеровский случайный процесс. Броуновское движение.
12. Технические каналы утечки информации. Демаскирующие признаки объектов защиты. Демаскирующие признаки объектов в видимом и ИК-диапазоне электромагнитного спектра. Демаскирующие признаки аналоговых и цифровых сигналов радиоэлектронных средств.
13. 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.
14. Физические основы возникновения акустического (виброакустического) канала утечки информации. Структура, классификация и основные характеристики акустических каналов утечки информации. Понятность и разборчивость речи. Средства акустической разведки.
15. 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.
16. Криптография на основе эллиптических кривых. Суть применения эллиптических кривых в криптографии.
17. Современные криптографические алгоритмы симметричной криптографии: ГОСТ 28147-89, AES. Архитектура, режимы использования.

18. Однонаправленные хеш-функции. Хеш-функции с ключом. Современные алгоритмы. Построение хеш-функции с использованием алгоритма шифрования.

19. Расстояние единственности. Понятие, возможности криптоанализа. Криптографические протоколы. Протокол Kerberos. Стандарт X.509

20. Инфраструктура открытых ключей (PKI) и удостоверяющие центры в корпоративных системах. Области применения криптографических методов. Построение VPN на PKI.

21. Основное назначение межсетевых экранов. Типы межсетевых экранов. Действия, осуществляемые межсетевым экраном в отношении трафика. Почему порядок правил в наборе правил межсетевого экрана играет важную роль? Преимущества и недостатки межсетевых экранов.

22. Основные устройства межсетевого взаимодействия. Основные составляющие эшелонированной обороны. Определение демилитаризованной зоны. Что такое сетевой периметр? Основные механизмы и службы защиты.

23. Безопасность сетевого оборудования. Принцип работы коммутатора и маршрутизатора. Методы обеспечения безопасности коммутаторов. Списки контроля доступа.

24. Понятие атаки на компьютерную систему. Основные угрозы при сетевом взаимодействии. Удалённая сетевая атака. Виды атак и их характеристика. 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).

25. 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? Основные составляющие обобщенного сценария атаки. Отличие атаки от вторжения. Что может быть установлено на атакуемой системе в результате успешной атаки? Оценивание степени серьезности атак.

26. Особенности атак на информационную систему при применении облачных технологий. Основные подходы к организации защиты информации в таких системах.

27. 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? Особенности биометрической аутентификации пользователей информационной системы.

28. 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.

29. 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.

30. Функции средств анализа защищённости компьютерных систем, их основные достоинства и недостатки. Сканирование уязвимостей, его ограниченность. Настройка и конфигурирование сканирования уязвимостей. Подготовка отчетов. Особенности сканирования уязвимостей.

31. Виды защищённого подключения к удалённым сетям. Безопасность виртуальных частных сетей. Технология работы VPN. Протоколы VPN. Режимы работы VPN.

32. Безопасность беспроводных сетей. Недостатки шифрования. Методы и рекомендации по повышению беспроводной сети. Основные принципы обнаружения вторжений в беспроводных сетях.

33. Задача идентификации пользователя. Понятие протокола идентификации. Локальная и удаленная идентификация. Идентифицирующая информация. Способы хранения идентифицирующей информации. Связь с ключевыми системами.

34. Модели разграничения доступа. Дискреционная модель. Мандатная модель. Реализация в ОС и средствах защиты информации.

35. Концепция защиты информации от НСД. Руководящие документы ФСТЭК по оценке защищенности от НСД. Государственные требования к построению СЗИ.

36. Подсистемы защиты современных операционных систем. Субъекты, объекты, методы и права доступа в современных операционных системах. Основные компоненты подсистем защиты операционных систем семейств UNIX и Windows.

37. Защита информации в вычислительных сетях и базах данных. Программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях;

38. Типовые решения в организации ключевых систем. Распределение ключей симметричного шифрования. Алгоритм DH.

39. Открытое распределение ключей. Распределение ключей асимметричного шифрования и ЭЦП. Ключевая система и ключевые носители СКЗИ «КриптоПро». Управление ключами СКЗИ «КриптоПро».

40. Механизм заражения программ вирусами. Необходимые и достаточные условия недопущения разрушающего воздействия. Понятие изолированной программной среды

ОСНОВНАЯ ЛИТЕРАТУРА

1. Ларина И.Е. Экономика защиты информации / Учебное пособие. - М.: МГИУ, 2007. 92 с.

2. Аверченков, В. И. Служба защиты информации : организация и управление [электронный ресурс] : учеб. пособие для вузов / В.И. Аверченков, М.Ю. Рытов. – 2-е изд., стереотип. – М. : ФЛИНТА, 2011. – 186 с.
3. Глухов М.М., Круглов И.А., Пичкур А.Б., Черемушкин А.В. Введение в теоретико-числовые методы криптографии. СПб: Лань, 2011. – 400 с.
4. 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.
5. Смирнов С.Н. Безопасность систем баз данных. Учебное пособие для вузов. М.: Гелиос-АРВ, 2007. – 351 с.
6. 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.
7. 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.
8. 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.
9. Хорев П.В. Программно-аппаратная защита информации: учебное пособие / П.Б. Хорев. – М.: ФОРУМ, 2009. – 352 с.

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. Участие в планировании и организации работ по обеспечению защиты информации: учебник / В.П. Зверева, А.В. Назаров. — М.: КУРС: ИНФРА-М, 2017. – 320 с.
6. Экономика индустриальных видов деятельности в России: Монография / С.В. Казаков, В.Я. Поздняков. - М.: НИЦ ИНФРА-М, 2014. – 304 с.
7. Экономика: Учебник / под ред. Липсиц И. В., 8-е изд., стер. – М.: Магистр, НИЦ ИНФРА-М, 2014. – 607 с.