МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Самарский государственный технический университет»
(ФГБОУ ВО «СамГТУ»)

УТВЕРЖДАЮ
Ректор ФГБОУ ВО «СамГТУ»
д.т.н., профессор
_____ Д.Е. Быков
«14» _____ 20 21 г.

ПРОГРАММА ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ В МАГИСТРАТУРУ

по направлению подготовки

10.04.01 Информационная безопасность
код и наименование направления подготовки

образовательная программа подготовки

«Информационная безопасность»
«Интеллектуальные средства в системах безопасности»
наименование образовательной программы подготовки

Самара 2021

1. ОБЩИЕ ПОЛОЖЕНИЯ

К вступительным испытаниям в магистратуру допускаются лица, имеющие документ государственного образца о высшем образовании любого уровня (диплом бакалавра, специалиста или магистра).

Лица, имеющие диплом магистра, могут быть зачислены только на места по договорам об оказании платных образовательных услуг.

Приём осуществляется на конкурсной основе по результатам вступительных испытаний.

Программа вступительных испытаний в магистратуру по направлению **10.04.01 Информационная безопасность** составлена на основании Федерального государственного образовательного стандарта высшего образования подготовки бакалавра по направлению **10.03.01 Информационная безопасность** и охватывает базовые дисциплины подготовки бакалавров по данному направлению подготовки.

Программа содержит описание формы вступительных испытаний, перечень вопросов для вступительных испытаний и список литературы рекомендуемой для подготовки.

2. ЦЕЛЬ ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ

Вступительные испытания призваны определить степень готовности поступающего к освоению основной образовательной программы магистратуры по направлению подготовки **Информационная безопасность,** образовательная программа **Интеллектуальные средства в системах безопасности**.

3. ФОРМА ПРОВЕДЕНИЯ И КРИТЕРИИ ОЦЕНКИ ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ

Вступительное испытание по профильным дисциплинам проводится в форме письменного экзамена в соответствии с установленным приёмной комиссией СамГТУ расписанием.

В билете содержится 6 вопросов

Критерии оценки вступительного испытания.

За каждый правильный ответ выставляется 17 баллов.

Максимальная оценка за тестовое задание — 100 баллов.

«Зачтено» - выставляется, если сформированность правильных ответов на тестовое задание составляет 40% (40 баллов) и более: поступающий показывает хорошие знания изученного учебного материала; самостоятельно интерпретирует материалы учебного курса; владеет основным терминами и понятиями изученного курса.

«Не зачтено» - выставляется, если сформированность правильных ответов на тестовое задание составляет менее 40%(40 баллов): при ответе поступающего выявились существенные проблемы в знаниях основных положений фактического материала.

Поступающему предлагается ответить письменно на вопросы теста в соответствии с экзаменационными заданиями, которые охватывают содержание разделов и тем программы соответствующих вступительных испытаний.

4. ПРОГРАММА ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ

Вступительное испытание по профильным дисциплинам проводится по программе, базирующейся на основной образовательной программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность.

Перечень разделов, тем дисциплины, вопросов и список литературы

ДИСЦИПЛИНА 1. Основы информационной безопасности

Перечень вопросов

1. Основные понятия и категории теории безопасности (понятия «опасность» и «безопасность», угрозы, риски, вызовы).
2. Основные понятия и категории теории безопасности (причины и последствия угроз безопасности, система обеспечения безопасности).
3. Информация, её виды и ценность.
4. Цели, задачи и ресурсы системы защиты информации.
5. Понятие о защищаемой информации.
6. Виды защищаемой информации.
7. Классификация демаскирующих признаков объектов защиты.
8. Видовые демаскирующие признаки.
9. Демаскирующие признаки сигналов.
10. Демаскирующие признаки веществ.
11. Методы определения количества информации.
12. Свойства информации, как предмета защиты (7 -определений).
13. Носители и источники информации.
14. Виды угроз безопасности информации.
15. Источники угроз безопасности информации (классификация несанкционированных угроз, структура разведывательных органов США).
16. Опасные сигналы и их источники.
17. Основные понятия информационной войны.
18. Определение информационного воздействия и информационного оружия.
19. Распределённые атаки на компьютерные сети - опасный вид информационного оружия.
20. Системы обнаружения информационных атак на компьютерные сети - оборонительное информационное оружие.
21. Системы контроля и перехвата информации в глобальных информационных сетях.
22. Классификация информационного оружия (виды, типы).
23. Классификация информационного оружия (по признакам, методам доставки).
24. Классификация информационного оружия (по способам воздействия).
25. Информационно-психологическое и энергоинформационное оружие (средства, воздействие на человека).
26. Перечень концептуальных документов, важнейших федеральных нормативно-правовых актов и основных подзаконных актов в области защиты информации.
27. Система государственных и отраслевых стандартов в области защиты информации.
28. Нормативные документы ФСТЭК РОССИИ.
29. Сертификация в области защиты информации (назначение и общая характеристика).
30. Сертификация в области защиты информации (добровольная сертификация).
31. Сертификация в области защиты информации (обязательное подтверждение соответствия).
32. Аттестация объектов информатизации.
33. Сертификация продукции, ввозимой из-за границы.
34. Политика информационной безопасности предприятия (назначение, содержание, структура).
35. Классификация технических каналов утечки информации.

36. Получение информации из печатных документов.
37. Получение информации из средств связи (радиоперехват).
38. Получение информации из средств связи (снятие информации с телефона).
39. Акустические каналы утечки информации.
40. Оптические каналы утечки информации.
41. Радиоэлектронные каналы утечки информации.
42. Вещественные каналы утечки информации.
43. Методы добывания информации.
44. Виды и методы технической защиты информации (общая характеристика, пассивная и активная защита).
45. Методы защиты от утечек по акустическим каналам (общая характеристика).
46. Защита средств связи и телекоммуникаций (методы).
47. Компьютерные вирусы (определение, классификация).
48. Криптографические средства защиты информации (основные понятия).
49. Криптографические средства защиты информации (шифрование с открытым ключом).
50. Криптографические средства защиты информации (шифрование с закрытым ключом).

ДИСЦИПЛИНА 2. Основы управления информационной безопасностью

Перечень вопросов

1. Понятие, предмет информационной безопасности и ее место в системе обеспечения национальной безопасности.
2. Основные положения Концепции национальной безопасности Российской Федерации и Доктрины информационной безопасности Российской Федерации.
3. Определение понятия «государственная тайна». Перечень сведений, составляющих государственную тайну.
4. Правовые механизмы отнесения сведений к государственной тайне, рассекречивания сведений и их носителей.
5. Защита государственной тайны. Субъекты защиты государственной тайны, их функции в данной сфере. Контроль и надзор за обеспечением защиты государственной тайны.
6. Особенности правовой защиты сведений, составляющих государственную тайну.
7. Основные объекты института коммерческой тайны.
8. Субъекты информационных правоотношений, возникающих по поводу коммерческой тайны.
9. Правовой режим коммерческой тайны.
10. Защита прав на коммерческую тайну. Ответственность за нарушения при работе с коммерческой тайной.
11. Институты профессиональных тайн и их значение для обеспечения защиты прав и свобод человека и гражданина, коммерческих интересов организаций и учреждений.
12. Основные категории сведений, защищаемых в режиме профессиональной тайны.
13. Система правового регулирования отдельных институтов профессиональных тайн.
14. Понятие и характеристика правонарушений в информационной сфере.
15. Криминалистическая характеристика преступлений в сфере компьютерной информации.
16. Ответственность за правонарушения в сфере компьютерной информации.
17. Сущность организационных методов защиты информации. Состояние организационных методов с правовыми и инженерно-техническими.

18. Организационные каналы передачи информации и каналы утечки информации и несанкционированного доступа к ней.
19. Совокупность методов защиты информации, используемых для перекрытия каналов утечки информации.
20. Система организационной защиты информации, составляющей государственную тайну.
21. Система организационной защиты конфиденциальной информации.
22. Установление и изменение степени секретности сведений, содержащихся в работах, документах, изделиях.
23. Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности.
24. Рассекречивание сведений, отнесенных к государственной тайне и конфиденциальных сведений.
25. Особенности подбора персонала на должности, связанные с работой с конфиденциальной информацией.
26. .Состав документов, необходимых при подборе и приеме сотрудников на должности, связанные с доступом к конфиденциальной информации,
27. Доступ к секретной информации.
28. Организация доступа к конфиденциальной информации.
29. Особенности лиц, допущенных к защищаемым сведениям.
30. Текущая работа с персоналом, обладающим конфиденциальной информацией.
31. Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации.
32. Факторы выбора приемов и средств охраны.
33. Контрольно-пропускные пункты, их оборудование и организация работы.
34. Режимные помещения и требования, предъявляемые к ним.
35. Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам.
36. Организация защиты информации при приеме в организации иностранных представителей.
37. Организация защиты информации при приеме в организации посетителей, командированных лиц.
38. Организация защиты информации при осуществлении рекламной деятельности.
39. Организация защиты информации при подготовке материалов к открытому опубликованию.
40. Технология аналитической работы.

ДИСЦИПЛИНА 3. Организационно-правовое обеспечение информационной безопасности

Перечень вопросов

1. Понятие, предмет информационной безопасности и ее место в системе обеспечения национальной безопасности.
2. Основные положения Концепции национальной безопасности Российской Федерации и Доктрины информационной безопасности Российской Федерации.
3. Определение понятия «государственная тайна». Перечень сведений, составляющих государственную тайну.
4. Правовые механизмы отнесения сведений к государственной тайне, рассекречивания сведений и их носителей.
5. Защита государственной тайны. Субъекты защиты государственной тайны, их функции в данной сфере. Контроль и надзор за обеспечением защиты государственной тайны.
6. Особенности правовой защиты сведений, составляющих государственную тайну.

7. Основные объекты института коммерческой тайны.
8. Субъекты информационных правоотношений, возникающих по поводу коммерческой тайны.
9. Правовой режим коммерческой тайны.
10. Защита прав на коммерческую тайну. Ответственность за нарушения при работе с коммерческой тайной.
11. Институты профессиональных тайн и их значение для обеспечения защиты прав и свобод человека и гражданина, коммерческих интересов организаций и учреждений.
12. Основные категории сведений, защищаемых в режиме профессиональной тайны.
13. Система правового регулирования отдельных институтов профессиональных тайн.
14. Понятие и характеристика правонарушений в информационной сфере.
15. Криминалистическая характеристика преступлений в сфере компьютерной информации.
16. Ответственность за правонарушения в сфере компьютерной информации.
17. Сущность организационных методов защиты информации. Соотношение организационных методов с правовыми и инженерно-техническими.
18. Организационные каналы передачи информации и каналы утечки информации и несанкционированного доступа к ней.
19. Совокупность методов защиты информации, используемых для перекрытия каналов утечки информации.
20. Система организационной защиты информации, составляющей государственную тайну.
21. Система организационной защиты конфиденциальной информации.
22. Установление и изменение степени секретности сведений, содержащихся в работах, документах, изделиях.
23. Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности.
24. Рассекречивание сведений, отнесенных к государственной тайне и конфиденциальных сведений.
25. Особенности подбора персонала на должности, связанные с работой с конфиденциальной информацией.
26. .Состав документов, необходимых при подборе и приеме сотрудников на должности, связанные с доступом к конфиденциальной информации,
27. Доступ к секретной информации.
28. Организация доступа к конфиденциальной информации.
29. Особенности лиц, допущенных к защищаемым сведениям.
30. Текущая работа с персоналом, обладающим конфиденциальной информацией.
31. Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации.
32. Факторы выбора приемов и средств охраны.
33. Контрольно-пропускные пункты, их оборудование и организация работы.
34. Режимные помещения и требования, предъявляемые к ним.
35. Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам.
36. Организация защиты информации при приеме в организации иностранных представителей.
37. Организация защиты информации при приеме в организации посетителей, командированных лиц.
38. Организация защиты информации при осуществлении рекламной деятельности.

39. Организация защиты информации при подготовке материалов к открытому опубликованию.
40. Технология аналитической работы.

ДИСЦИПЛИНА 4. Программно-аппаратные средства защиты информации
Перечень вопросов

1. Аппаратные средства защиты информации. Аппаратные токены ЭЦП.
2. Аппаратные токены ЭЦП. Основные механизмы. Удостоверяющие центры. Инструменты.
3. Работа с крипто провайдерами КриптоПроCSP и носителями ЭЦП. Использование КриптоПро CSP в ПО Microsoft. Цели использования криптографических функций.
4. Биометрические системы защиты. Сканеры. Голосовая идентификация.
5. Средства организации виртуальных частных сетей. Задачи решаемые VPN.
6. Средства организации виртуальных частных сетей. Туннелирование VPN. Уровни защищенных каналов.
7. Защита данных на сетевом уровне. Протокол SKIP. Протокол IPSec.
8. Источники функциональных сигналов. Радиопередатчики и радиотехнические средства и системы.
9. Обнаружение и локализация закладных устройств. Способы локализации.
10. Уязвимости и угрозы безопасности ПО. Уязвимости ПО. Классификация уязвимостей ПО.
11. Угрозы безопасности ПО. Уязвимость информационной системы. "Окно опасности". Классификация угроз
12. Несанкционированное исследование и копирование программ. Классификация средств несанкционированного исследования программ.
13. Методы тестирования программного обеспечения на его защищенность. Методы тестирования программ.
14. Фаззинг программ. Фаззинг тест. Алгоритм работы.
15. Методы защиты программ от несанкционированного исследования. Способы защиты от несанкционированного исследования программ и их классификация.
16. Обфускация программ. Обфускация структур данных.
17. Обфускация программ. Обфускация потока управления.
18. Обфускация программ. Превентивная Обфускация.
19. Обфускация программ. Лексическая Обфускация.
20. Методы защиты программ от несанкционированного копирования. Криптографические методы.
21. Использование Microsoft Cryptographic API (CryptoAPI). Модуль шифрования PGP.
22. Методы защиты программ от несанкционированного копирования. Метод привязки к идентификатору.
23. Методы защиты программ от несанкционированного копирования. Манипуляции с кодом программы.
24. Защищённые операционные системы. Состав дистрибутива ОС Linux с повышенными требованиями к ее защищённости.
25. Вредоносное программное обеспечение. Классификация вредоносных программ.
26. Вредоносное программное обеспечение. Троянские программы.
27. Компьютерные вирусы. Структура, жизненный цикл и принцип работы вируса.
28. Компьютерные вирусы. Классификация компьютерных вирусов.
29. Компьютерные вирусы. Сетевые вирусы.
30. Компьютерные вирусы. Прочие вредоносные программы.
31. Защита от вредоносных программ. Антивирусные программы.

32. Защита от вредоносных программ. Детекторы.
33. Защита от вредоносных программ. Технологии проактивной защиты.
34. Строение и выделение оперативной памяти в MS-DOS. Резидентность.
35. Резидентные COM и EXE вирус.
36. Загрузочный вирус. Файлово-загрузочный вирус.
37. Антивирус, сканирующий диск, память и загрузочные области.
38. Программы типа COM, EXE. Формат заголовка EXE. Структура PSP.
39. Функции MS-DOS для работы с клавиатурой, монитором и файлами.
40. Формат команд. Кодирование регистров и условных переходов.
41. Архитектура памяти. Таблица векторов прерываний. Перехват прерываний.
42. Загрузка ЭВМ. Организация жесткого диска. MBR и таблица разделов.

ДИСЦИПЛИНА 5. Криптографические методы защиты информации
Перечень вопросов

1. Предмет криптографии. Определения. Задачи. Исторические примеры.
2. Классическая задача криптографии. Задача идентификации авторства сообщения.
3. Виды атак на криптографические алгоритмы. Понятие стойкости.
4. Классификация алгоритмов шифрования. Примеры простейших шифров.
5. Шифры замены и перестановки. Примеры.
6. Моно- и многоалфавитные подстановки. Перестановочные шифры. Примеры.
7. Простой столбцевой перстановочный шифр. Примеры.
8. Перестановочный шифр с ключевым словом. Примеры.
9. Подстановочные шифры. Шифр Атбаш. Примеры.
10. Подстановочные шифры. Квадрат Полибия. Примеры.
11. Подстановочные шифры. Шифр Сцитала. Примеры.
12. Подстановочные шифры. Шифр Цезаря. Примеры.
13. Подстановочные шифры. Шифр Цезаря с ключевым словом. Примеры.
14. Подстановочные шифры. Шифр Тритемия. Примеры.
15. Подстановочные шифры. Шифр Виженера с перемешанным один раз алфавитом. Примеры.
16. Подстановочные шифры. Шифр с автоключём. Примеры.
17. Подстановочные шифры. Шифр Плейфера. Двойной квадрат. Примеры.
18. Шифровальные машины. Шифр Хилла.
19. Методы анализа многоалфавитных систем.
20. Классификация методов дешифрования.
21. Модель предполагаемого противника.
22. Совершенная секретность по Шеннону. Примеры совершенно секретных систем.
23. Криптография открытых ключей. Проблема перехвата ключей. Простые числа
24. Криптография открытых ключей. Алгоритм Диффи-Хеллмана.
25. Понятие об управлении ключами.
26. Блочные криптосистемы с секретным ключом.
27. Блочные криптосистемы с секретным ключом. Описание S - DES. Основные этапы алгоритма.
28. Блочные криптосистемы с секретным ключом. Алгоритм шифрования УАШ.
29. Блочные криптосистемы с секретным ключом. Алгоритм шифрования S- AES.
30. Хэш функция. Алгоритм MD5.
31. Электронные цифровые подписи. Стандарт DSS.
32. Криптографические протоколы. Понятие криптографического протокола.
33. Криптоанализ. Обзор возможных вариантов криптоанализа.
34. Методы криптоанализа симметричных криптосистем.
35. Перехват открытых ключей. Алгоритм Диффи-Хеллмана.

36. Частотный метод криптоанализа симметричных криптосистем.
37. Принципы стеганографии.
38. История стеганографии. Принципы стеганографии.
39. Методы стеганографии. Лексический метод.
40. Методы стеганографии. Метод встраивания скрытой информации в графический файл.

ДИСЦИПЛИНА 6. Техническая защита информации

Перечень вопросов

1. Технические каналы утечки информации.
2. Высокочастотные опасные излучения.
3. Основные технические средства и вспомогательные технические средства.
4. Процедуры обнаружения и распознавания.
5. Контролируемая зона.
6. Показатели качества подслушиваемой речи.
7. Основные виды каналов утечки информации, обрабатываемой ТСПИ.
8. Разборчивость речи.
9. Побочные электромагнитные излучения.
10. Показатели эффективности добывания информации.
11. Электрические каналы утечки информации.
12. Виды радиоэлектронных каналов утечки информации.
13. Закладные устройства.
14. Показатели метеорологической дальности видимости.
15. Каналы утечки речевой информации.
16. Явление реверберации.
17. Метод «высокочастотного навязывания».
18. Классификация каналов утечки информации.
19. Лазерный канал утечки информации.
20. Характеристики речевой информации.
21. Метод «высокочастотного облучения».
22. Утечка информации по цепям заземления.
23. Основные виды каналов утечки информации, передаваемой по каналам связи.
24. Опасные сигналы в цепях электропитания.
25. Способы получения видовой информации.
26. Случайные акустоэлектрические преобразователи.
27. Принципы организации несанкционированного доступа к информации.
28. Экранирование электромагнитных полей.
29. Программные закладки.
30. Назначение и основные задачи, решаемые комплексом «Навигатор».
31. Каналы утечки информации при работе средств вычислительной техники.
32. Фильтрация опасных сигналов.
33. Зона возможного перехвата информации.
34. Основной метод защиты информации в радиоканалах связи.
35. Основные акустические параметры речевых сигналов.
36. Активные способы защиты от опасных сигналов.
37. Методы скрытия и закрытия информации.
38. Методы звукоизоляции и звукопоглощения.
39. Индикаторы поля, частотомеры.
40. Метод физического подавления закладных устройств.
41. Принципы построения индикаторов поля.
42. Метод синфазной низкочастотной помехи.
43. Основные характеристики радиоприемных устройств.
44. Метод ультразвуковой маскирующей помехи.
45. Радиоприемные устройства ближней зоны.
46. Метод маскирующей высокочастотной помехи.
47. Сканирующие приемники.

48. Условия эффективного энергетического скрытия.
49. Первичные и вторичные источники информации.
50. Основные источники угроз информации, содержащей государственную тайну.
51. Ценность и цена информации.
52. Основные источники опасных случайных сигналов.

Основная учебная литература

1. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Основы управления информационной безопасностью. Учебное пособие для вузов. – 2-е изд., испр. – М.: Горячая линия-Телеком, 2019. – 244.: ил.
2. Башлы П.Н. Информационная безопасность и защита информации: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова Е.К.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2012.— 311 с.
3. Титов А.А. Инженерно-техническая защита информации: учебное пособие/ А.А. Титов— Электрон. текстовые данные.— Томск: Томский государственный университет систем управления и радиоэлектроники, 2010.— 197 с.
4. Шаньгин В.Ф. Информационная безопасность и защита информации / Шаньгин В.Ф.— Электрон. текстовые данные.— М.: ДМК Пресс, 2014.— 702 с.
5. Управление безопасностью : учеб. пособие / Л. П. Гончаренко, Е. С. Куценко; Рос. экон. акад. им. Г. В. Плеханова.- М.: КноРус, 2010. - 272 с.
6. Инженерно-техническая защита информации: Учеб. пособие для вузов / А. А. Торокин.- М.: Гелиос АРВ, 2006. -958 с.
7. Информационное обеспечение управленческой деятельности: учеб. пособие для сред. спец. образования / Е. Е. Степанова, Н. В. Хмелевская.- М.: Форум , 2010. - 191 с.
8. Ищейнов В.Я., Мецатунян М.В. Защита конфиденциальной информации. – Форум, 2009. – 256 с.
9. Клейменов С.А., Мельников В.П., Петраков А.М. Информационная безопасность и защита информации: учеб. пособие. – Академия, 2008. – 336 с.
10. Ковалева Н.Н. Информационное право России: учеб. пособие / Н.Н. Ковалева. – М.: Дашков и К, 2007. – 358 с.
11. Краковский Ю.М. Информационная безопасность и защита информации. – ИЦ МарТ ИКЦ МарТ, 2008. – 288 с.
12. Правовое обеспечение информационной безопасности: учебник / [авт.-ред.: В.А. Минаев и др.]. – Изд. 2-е, расш. и доп. – М.: Маросейка, 2008. – 368 с.
13. Программно-аппаратная защита информации [Текст] : учеб. пособие по направлениям "Информ. безопасность" и "Информатика и вычисл. техника" / П. Б. Хорев.- М. : Форум , 2009.-351
14. Организационное обеспечение информационной безопасности : учебник для высш. учеб. заведений по направлению "Информационная безопасность" / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М.: Академия, 2008.-188 с.
15. Теоретические основы компьютерной безопасности: учеб. пособие для вузов по специальности 090100 "Информационная безопасность" / А.А. Грушо, Э.А. Применко, Е. Е. Тимонина. - М.: Академия, 2009. - 267 с.
16. Информационная безопасность и защита информации : учеб. пособие для студентов вузов по направлению 230200 "Информ. системы" специальности 230201 "Информ. системы и технологии" / Ю. Ю. Громов и др. - Старый Оскол: Тонкие наукоемкие технологии, 2010. - 383 с.
17. Тилборг Ван Х.К.А. Основы криптологии. Профессиональное руководство и интерактивный учебник [Текст] / Х. К. А. ван Тилборг ; пер. с англ. Д. С. Ананичева, И. О. Корякова ; под ред. И. О. Корякова. - М.: Мир, 2006.
18. Торстейнсон, П. Криптография и безопасность в технологии. NET [Текст] / П. Торстейнсон, Г. А. Ганеш ; пер. с англ. В. Д. Хорева ; под ред. С. М. Молявко.- М. : Бином.

Лаборатория знаний , 2007.-479 с.

19. Фороузан, Б. А. Криптография и безопасность сетей: учеб. пособие / Б. А. Фороузан ; пер. с англ. под ред. А. Н. Берлина.- М.: Интернет-Университет Информационных Технологий: БИНОМ. Лаборатория знаний, 2010. - 783 с.

Дополнительная учебная литература

1. Галатенко В.А. Основы информационной безопасности/ Галатенко В.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2008.— 174 с.

2. ГОСТ Р-50922-2006. Защита информации. Основные термины и определения. М.: Госстандарт России, 2006.

3. Аникин П.П., Балыбердин А.Л., Вус М.А. Государственная тайна и ее защита в Российской Федерации: учеб. пособие (под ред. Вуса М.А., Федорова А.В.; предисл. Кропачева Н.М., Сидоровой Н.А.). – Изд. 2-е, перераб., доп. –изд-во Р. Асланова «Юридический Центр-Пресс«, 2005. – 623 с.

4. Правовое обеспечение информационной безопасности: учеб. пособие / под ред. С.Я. Казанцева. – 2-е изд., испр. и доп. – М.: Академия, 2007. – 238 с.

5. Компьютерные вирусы изнутри и снаружи / К. Касперски. .- СПб. и др. : Питер , 2007.-526 с.

6. Шаффер, М. Защита от шума и вибраций в системах ОВК: практ. руководство: пер. с англ. / М. Шаффер.- М.: Авок-Пресс, 2009.-231 с.

7. Панасенко С.П. Алгоритмы шифрования. Специальный справочник. – СПб.: БХВ-Петербург, 2009.-564 с.

5. ДЕМОНСТРАЦИОННЫЙ ВАРИАНТ ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ

Вариант 1

1. Основные понятия и категории теории безопасности (понятия «опасность» и «безопасность», угрозы, риски, вызовы).
2. Понятие, предмет информационной безопасности и ее место в системе обеспечения национальной безопасности.
3. Организация защиты информации при приеме в организации иностранных представителей.
4. Аппаратные средства защиты информации. Аппаратные токены ЭЦП.
5. Частотный метод криптоанализа симметричных криптосистем.
6. Технические каналы утечки информации.

Вариант 2

1. Основные понятия и категории теории безопасности (причины и последствия угроз безопасности, система обеспечения безопасности).
2. Основные положения Концепции национальной безопасности Российской Федерации и Доктрины информационной безопасности Российской Федерации.

3. Организация защиты информации при приеме в организации посетителей, командированных лиц.
4. Аппаратные токены ЭЦП. Основные механизмы. Удостоверяющие центры. Инструменты.
5. Принципы стеганографии.
6. Высокочастотные опасные излучения.

Вариант 3

1. Информация, её виды и ценность.
2. Определение понятия «государственная тайна». Перечень сведений, составляющих государственную тайну.
3. Организация защиты информации при осуществлении рекламной деятельности.
4. Работа с крипто провайдерами КриптоПроCSP и носителями ЭЦП. Использование КриптоПро CSP в ПО Microsoft. Цели использования криптографических функций.
5. История стеганографии. Принципы стеганографии.
6. Основные технические средства и вспомогательные технические средства.

Вариант 4

1. Цели, задачи и ресурсы системы защиты информации.
2. Правовые механизмы отнесения сведений к государственной тайне, рассекречивания сведений и их носителей.
3. Организация защиты информации при подготовке материалов к открытому опубликованию.
4. Биометрические системы защиты. Сканеры. Голосовая идентификация.
5. Методы стеганографии. Лексический метод.
6. Процедуры обнаружения и распознавания.

Вариант 5

1. Понятие о защищаемой информации.
2. Защита государственной тайны. Субъекты защиты государственной тайны, их функции в данной сфере. Контроль и надзор за обеспечением защиты государственной тайны.
3. Технология аналитической работы.
4. Средства организации виртуальных частных сетей. Задачи решаемые VPN.
5. Методы стеганографии. Метод встраивания скрытой информации в графический файл.
6. Контролируемая зона.