МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
“УЛЬЯНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ”
ИНСТИТУТ ЭКОНОМИКИ И БИЗНЕСА

Нуретдинова Ю.В.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ПО ДИСЦИПЛИНЕ «ИНФОРМАЦИОННО-УЧЕТНОЕ ОБЕСПЕЧЕНИЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ»

Ульяновкс 2019

Методические указания для самостоятельной работы студентов по дисциплине “Информационно-учетное обеспечение экономической безопасности ” / составитель Ю.В.Нуретдинова, - Ульяновск: УлГУ, 2019. – 27с.

Настоящие методические указания предназначены для студентов экономических направлений и специальностей всех форм обучения, изучающих дисциплину «Информационно-учетное обеспечение экономической безопасности)» В работеприведена литература по дисциплине, основные темы курса и вопросы в рамках каждой темы, рекомендации по изучению теоретического материала, контрольные вопросы для самоконтроля и тесты для самостоятельной работы.

Студентам заочной формы обучения следует использовать данные методические указания при самостоятельного изучения дисциплины. Студентам очной формы обучения они будут полезны при подготовке к практическим занятиям и к зачеты по данной дисциплине.

Рекомендованы к использованию ученым советом
Института экономики и бизнеса УлГУ
Протокол № 222/08 от « 23» мая 2019г.

I. ЛИТЕРАТУРА ДЛЯ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

а) основная литература:

1.Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для бакалавриата и магистратуры / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2019. — 342 с. — (Бакалавр и магистр. Модуль). — ISBN 978-5-534-05142-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/441287

2.Экономическая безопасность : учебник для вузов / Л. П. Гончаренко [и др.] ; под общей редакцией Л. П. Гончаренко. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2019. — 340 с. — (Специалист). — ISBN 978-5-534-06090-4. — Режим доступа : www.biblio-online.ru/book/ekonomicheskaya-bezopasnost-432165

б) дополнительная литература:

1.Организационное и правовое обеспечение информационной безопасности: учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2019. — 325 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/432966

в) учебно-методическая литература:

1.Методические указания по организации самостоятельной работы студентов специальности 38.05.01 «Экономическая безопасность» специализация «Финансовый учет и контроль в правоохранительных органах» для всех форм обучения, Составитель Романова И.Б., Ермишина О.Ф.: УлГУ. Институт Экономики и Бизнеса. - Ульяновск, 2019. – 62 с.

II. МЕТОДИЧЕСКИЕ УКАЗАНИЯ

Тема 1. Основные понятия и определения информационной безопасности

Вопросы:

1. Основные понятия и определения.
2. Понятия информация, информатизация, информационная система, информационная безопасность.
3. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене.
4. Защита информации, тайна, средства защиты информации.
5. Международные стандарты информационного обмена.
6. Показатели информации: важность, полнота, адекватность, релевантность, толерантность.
7. Требования к защите информации.
8. Комплексность системы защиты информации: инструментальная, структурная, функциональная, временная

Рекомендации по изучению темы:

Вопрос 1,2,3,4 темы следует изучить по учебнику 1 и 2 основной литературы.
Вопрос 5,6 изложен в учебнике 1 дополнительной литературы.
Для самостоятельного изучения вопроса 7,8 следует обратиться к учебнику 1 дополнительной литературы.

Контрольные вопросы:

1. Определить место информационной безопасности в обеспечении системы общественной безопасности.
2. Дать определение информационной безопасности.
3. Назвать основные направления и задачи обеспечения информационной безопасности общества.
4. Назвать основные компоненты информационной безопасности автоматизированных информационных систем.
5. Охарактеризовать уровни реализации информационной безопасности.
6. Дать определение и классификацию информационных ресурсов.
7. Определить основные виды угроз информационным ресурсам.
8. Охарактеризовать особенности угроз конфиденциальной информации

Ответьте на тестовые вопросы:

1.Что такое информационная безопасность, каковы ее основные аспекты?

1.Информационная безопасность – это целостность данных, доступность информации для всех авторизованных пользователей и ее конфиденциальность.

2. Информационная безопасность – многогранная область деятельности, в которой успех может принести только комплексный подход.
3. Информационная безопасность – составная часть информационных технологий.
4. Информационная безопасность – защищенность потребностей объекта в качественной информации, необходимой ему для нормального функционирования и развития.

2. Укажите основные законы, относящиеся к организации и функционированию системы информационной безопасности и защиты информации.

1. «Об информации, информационных технологиях и защите информации» от 27.07.2006 №149-ФЗ.
2. «Об информации, информатизации и защите информации» от 20.02.95 №24-ФЗ.
3. «О товарных знаках, знаках обслуживания и наименования мест происхождения товаров» от 23.09. №3520-1.
4. «Об электронной цифровой подписи» от 10.01.2002 №1-ФЗ.

3. Каковы основные задачи в сфере обеспечения информационной безопасности? (несколько вариантов):

1. Развитие стандартизации информационных систем на базе общепризнанных международных стандартов и их внедрение для всех видов информационных систем.
2. Противодействие угрозе развязывания противоборства в информационной сфере.
3. Организация международного сотрудничества по обеспечению информационной безопасности при интеграции России в мировое информационное пространство.
4. Совершенствование и защита отечественной информационной структуры, ускорение развития новых информационных технологий и их широкое распространение с учетом вхождения России в глобальную информационную инфраструктуру.

4. Что такое политика безопасности?

1.Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации.

2. Политика безопасности отвечает реальным рискам организации.
3. Политика безопасности состоит из трех уровней.
4. Первый уровень безопасности самый общий.

5.Что такое государственная тайна?

1. Защищаемые государством сведения в области его военной, внешне-политичекой, экономической, контрразведывательной, оперативно-розыскной деятельности.
2. Сведения, которые отвечают определенным требованиям.
3. Информация коммерческих структур.
4. Сведения, не подлежащие засекречиванию.

6. Что такое коммерческая тайна?

1. Информация может составлять коммерческую тайну, если она отвечает определенным требованиям.
2. Сведения, отвечающие законодательству РФ к коммерческой тайне.
3. Информация, являющаяся собственностью государственных структур.
4. Сведения, которые не могут быть отнесены к государственной тайне.

7. Что такое служебная тайна?

1. Служебная информация о деятельности государственных организаций.
2. Охраняемые государством сведения в любой области науки, техники, производства и управления, разглашение которых может нанести ущерб интересам государства.
3. Информация, которая не является государственной тайной.
4. Информация, которая не может быть отнесена к служебной тайне.

8. Что такое профессиональная тайна?

1. Защищаемая по закону информация, доверенная или ставшая известной лицу исключительно в Сулу исполнения им своих профессиональных обязанностей.
2. Если она отвечает охраноспособности права.
3. Информация, распространение которой может нанести ущерб правам доверителя.
4. Информация не являющаяся государственной или коммерческой тайной.

9.Что такое персональные данные?

1. Любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных).
2. Конфиденциальная информация, перечень которой закреплен Федеральным законом.
3. Биографические и опознавательные данные (в том числе об обстоятельствах рождения, усыновления, развода).
4. Сведения об имущественном, финансовом положении и о состоянии здоровья.

10. Что такое источники права на доступ к информации?

1. Наряду с Конституцией РФ источниками права о доступе к информации является: законы, подзаконные, нормативные акты, международные правовые акты, договоры и соглашения.
2. Государственные информационные ресурсы на доступ к которым не требуется обосновывать необходимость получения запрашиваемой информации.
3. Информация, полученная на законных основаниях из государственных информационных ресурсов.

4. Информационное обеспечения пользователей по вопросам прав, свобод и обязанностей граждан, их безопасности и др. вопросам представляющим общественный интерес.

Тема 2. Государственная система информационной безопасности

Вопросы:

1. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
2. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.
3. Доктрина информационной безопасности Российской Федерации.
4. Структура государственной системы информационной безопасности.
5. Структура законодательной базы по вопросам информационной безопасности.
6. Лицензирование и сертификация в области защиты информации.
7. Место информационной безопасности экономических систем в национальной безопасности страны.
8. Концепция информационной безопасности.

Рекомендации по изучению темы:

Вопрос 1,3,5,7 темы следует изучить по учебнику 1 и 2 основной литературы.
Вопрос 2,4,6 изложен в учебнике 1 дополнительной литературы.
Для самостоятельного изучения вопроса 8 следует обратиться к учебнику 1 основной литературы.

Контрольные вопросы:

1. Проанализировать основные направления правовой защиты информации.
2. Раскрыть содержание нормативных актов, защищающих право граждан на своевременное получение достоверной информации.
3. Изложить законный порядок реализации права гражданина на опровержение ложной информации о нем в средствах массовой информации.
4. Показать порядок защиты прав граждан на личную тайну и неприкосновенность частной жизни законодательством Российской Федерации о СМИ.
5. Определить объекты защиты авторских прав.
6. Назвать основные права автора в отношении его произведения.
7. Определить объекты интеллектуальной собственности, защищаемые патентным законодательством.
8. Охарактеризовать основные права патентообладателя в отношении его произведения (промышленного образца, полезной модели).
9. Дать определение государственной тайны и назвать грифы секретности.
10. Перечислить сведения, составляющие государственную тайну и сведения, которые не могут относиться к государственной тайне.
11. Изложить порядок отнесения сведений к государственной тайне и их засекречивания.
12. Раскрыть последовательность условия и формы допуска должностных лиц к государственной тайне.
13. Дать определение коммерческой тайны и перечислить сведения, которые не могут быть ее объектом.
14. Охарактеризовать порядок установления режима коммерческой тайны и основные права ее субъектов.

15. Назвать основные виды служебной тайны определенные законодательством Российской Федерации

Ответьте на тестовые вопросы:

11. Информация, к которой нельзя ограничивать доступ? (несколько вариантов):
    1. Информация о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну.
    2. Информация о состоянии окружающей среды.
    3. Коммерческая тайна.
    4. Банковская тайна.
12. Что такое информация с ограниченным доступом?
    1. Информация, доступ к которой ограничен федеральными законами
    2. Закон о коммерческой тайне.
    3.Информация, полученная на законных основаниях из государственных информационных ресурсов.
    4. Сведения об имущественном, финансовом положении и о состоянии здоровья.
13. Что такое надежность информации?
    1. Под надежностью информации понимается интегральный показатель, характеризующий ее целостность, отсутствие в ней подмены.
    2. Комплекс мер по защите информации в ходе непрерывного процесса подготовки, обработки, хранения и передачи информации.
    3. Безопасность информации.
    4.Уверенность в том, что преданные владельцем данные не будут размножаться, копироваться и использоваться без его санкции.
14. В чем заключается уязвимость информации?
    1. Заключается в нарушении ее физической сохранности, структурной целостности, доступности для правомочных пользователей..
    2. Современные АС могут быть объектом случайных и умышленных воздействий.
    3. Вероятность нарушения защищаемых характеристик АС.
    4. В наличие и количестве дестабилизирующих факторов, потенциально возможных в структурных компонентов автоматизированных систем.
15. Сложность обеспечения информационной безопасности является следствием:
    1. Злого умысла разработчиков информационных систем
    2. Объективных проблем современной технологии программирования
    3. Происков западных спецслужб, встраивающих "закладки" в аппаратуру и программы
16. В число универсальных сервисов безопасности входят:
    1. "разделяй и властвуй"
    2. разделение обязанностей
    3. инкапсуляция наследования
    4. Метод «запрос-»
17. Комплексное экранирование может обеспечить (несколько вариантов):
    1. разграничение доступа по сетевым адресам
    2. выборочное выполнение команд прикладного протокола
    3. контроль объема данных, переданных по TCP-соединению
18. Перехват данных является угрозой:

1. доступности
2. конфиденциальности
3. целостности
4. защиты от копирования

19. Что из перечисленного не относится к числу основных аспектов информационной безопасности:

1.доступность
2. целостность
3. защита от копирования
4. конфиденциальность

20. В число целей политики безопасности верхнего уровня входят (несколько вариантов):

1. формулировка административных решений по важнейшим аспектам
2. реализации программы безопасности
3. выбор методов аутентификации пользователей обеспечение базы для соблюдения законов и правил

Тема 3. Теоретические основы угроз информационной безопасности

Вопросы:

1. Основные положения теории информационной безопасности информационных систем.
2. Модели безопасности и их применение.
3. Понятие угрозы. Виды противников или «нарушителей».
4. Классификация угроз информационной безопасности. Виды угроз.
5. Основные нарушения. Характер происхождения угроз (умышленные и естественные факторы).
6. Источники угроз. Предпосылки появления угроз.
7. Классы каналов несанкционированного получения информации. Причины нарушения целостности информации.

Рекомендации по изучению темы:

Вопрос 1,3,7 темы следует изучить по учебнику 1 и 2 основной литературы.
Вопрос 2,4, изложен в учебнике 1 дополнительной литературы.
Для самостоятельного изучения вопроса 5,6 следует обратиться к учебнику 1 основной литературы.

Контрольные вопросы:

1. Определить основные виды угроз информационным ресурсам.
2. Охарактеризовать особенности угроз конфиденциальной информации.
3. Проанализировать причины возникновения угроз утраты или утечки конфиденциальной информации.
4. Описать причины возникновения каналов несанкционированного доступа к информации.
5. Классифицировать виды каналов несанкционированного доступа к информации.

6. Описать характер действия организационных каналов несанкционированного доступа к информации.
7. Охарактеризовать технические каналы несанкционированного доступа к информации.
8. Охарактеризовать легальные и нелегальные методы обеспечения действия каналов утечки информации.
9. Проанализировать особенности угроз автоматизированным информационным системам.
10. Дать классификацию удаленных атак.

Ответьте на тестовые вопросы:

21. В число граней, позволяющих структурировать средства достижения информационной безопасности, входят:

1. законодательные меры
2. меры обеспечения доступности
3.профилактические меры
4. совокупность целей безопасности

22. В число этапов управления рисками входят (несколько вариантов):

1. анализ угроз
2. угрозы проведения анализа
3. выявление уязвимых мест

23. Агрессивное потребление ресурсов является угрозой:

1. доступности
2. конфиденциальности
3. целостности
4. защиты от копирования

24. В рамках программы безопасности нижнего уровня определяются:

1. совокупность целей безопасности
2. набор используемых механизмов безопасности
3. наиболее вероятные угрозы безопасности
4. совокупность целей безопасности

25. Что из перечисленного относится к числу основных аспектов информационной безопасности:

1.подотчетность - полнота регистрационной информации о действиях субъектов
2. приватность - сокрытие информации о личности пользователя
3. конфиденциальность - защита от несанкционированного ознакомления

26.Охрана персональных данных, государственной, служебной и других видов информации ограниченного доступа это:

1. Защита информации
2. Компьютерная безопасность
3. Защищенность информации
4. Защищенность потребителей информации
5. Безопасность данных

27. Создание и использование средств опасного воздействия на информационные сферы других стран мира и нарушение нормального функционирования информационных и телекоммуникационных систем это:

1. Информационная война
2. Информационное оружие
3. Информационное превосходство

28. Реализация конституционных прав и свобод человека, обеспечение личной безопасности, повышение качества и уровня жизни это:

1. Интересы государства
2. Интересы государства в информационной сфере
3. Интересы личности
4. Интересы личности в информационной сфере
5. Интересы общества в информационной сфере

29. Информация, не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения, в преимущественное положение по сравнению с другими объектами:

1. Служебная информация
2. Коммерческая тайна
3. Банковская тайна
4. Конфиденциальная информация

30. Действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости системы.

1. Комплексное обеспечение информационной безопасности
2. Безопасность АС
3. Угроза информационной безопасности
4. Атака на автоматизированную систему
5. Политика безопасности
6. конфиденциальность

Тема 4. Методы обеспечения информационной безопасности

Вопросы:

1. Использование защищенных компьютерных систем.
2. Аппаратные и программные средства для защиты компьютерных систем от НСД. Средства операционной системы.
3. Средства резервирования данных.
4. Проверка целостности.
5. Способы и средства восстановления работоспособности.

Рекомендации по изучению темы:

Вопрос 1,3 темы следует изучить по учебнику 1 и 2 основной литературы.
Вопрос 2,4 изложен в учебнике 1 дополнительной литературы.
Для самостоятельного изучения вопроса 5 следует обратиться к учебнику 1 основной литературы.

Контрольные вопросы:

1. Основные меры по обеспечению информационной безопасности Российской Федерации в сфере экономики?

2. Наиболее важные объекты обеспечения информационной безопасности Российской Федерации в области науки и техники?
3. Ограничение доступа как метод обеспечения информационной безопасности?
4. Биометрические методы аутентификации человека?
5. Статистика применения биометрических технологий?
6. Отпечатки пальцев как биометрическая характеристика идентификации человека?
7. Глаза как биометрическая характеристика идентификации человека?
8. Лицо как биометрическая характеристика идентификации человека?
9. Ладонь как биометрическая характеристика идентификации человека?
10. Динамические характеристики как биометрическая характеристика идентификации человека?
11. Классификация систем тревожной сигнализации?
12. Контроль доступа к аппаратуре как метод обеспечения информационной безопасности?
13. Разграничение и контроль доступа к информации как метод обеспечения информационной безопасности?
14. Предоставление привилегий на доступкак метод обеспечения информационной безопасности?
15. Защита информации от утечки за счет побочного электромагнитного излучения и наводок?
16. Методы и средства защиты информации от побочного электромагнитного излучения и наводок информации?
17. Методы и средства защиты информации от случайных воздействий?
18. Методы защиты информации от аварийных ситуаций?
19. Организационные мероприятия по защите информации?
20. Организация информационной безопасности компании?
21. Информационное страхование?

Ответьте на тестовые вопросы:

1.Что такое информационная безопасность, каковы ее основные аспекты?

1.Информационная безопасность – это целостность данных, доступность информации для всех авторизованных пользователей и ее конфиденциальность.

2. Информационная безопасность – многогранная область деятельности, в которой успех может принести только комплексный подход.

3. Информационная безопасность – составная часть информационных технологий.

4. Информационная безопасность – защищенность потребностей объекта в качественной информации, необходимой ему для нормального функционирования и развития.

2. Укажите основные законы, относящиеся к организации и функционированию системы информационной безопасности и защиты информации.

1. «Об информации, информационных технологиях и защите информации» от 27.07.2006 №149-ФЗ.

2. «Об информации, информатизации и защите информации» от 20.02.95 №24-ФЗ.

3. «О товарных знаках, знаках обслуживания и наименования мест происхождения товаров» от 23.09. №3520-1.

4. «Об электронной цифровой подписи» от 10.01.2002 №1-ФЗ.

3. Каковы основные задачи в сфере обеспечения информационной безопасности? (несколько вариантов):

1. Развитие стандартизации информационных систем на базе общепризнанных международных стандартов и их внедрение для всех видов информационных систем.
2. Противодействие угрозе развязывания противоборства в информационной сфере.
3. Организация международного сотрудничества по обеспечению информационной безопасности при интеграции России в мировое информационное пространство.
4. Совершенствование и защита отечественной информационной структуры, ускорение развития новых информационных технологий и их широкое распространение с учетом вхождения России в глобальную информационную инфраструктуру.

4. Что такое политика безопасности?

1.Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации.
2. Политика безопасности отвечает реальным рискам организации.
3. Политика безопасности состоит из трех уровней.
4. Первый уровень безопасности самый общий.

5.Что такое государственная тайна?

1. Защищаемые государством сведения в области его военной, внешне-политичекой, экономической, контрразведывательной, оперативно-разыскной деятельности.
2. Сведения, которые отвечают определенным требованиям.
3. Информация коммерческих структур.
4. Сведения, не подлежащие засекречиванию.

6. Что такое коммерческая тайна?

1. Информация может составлять коммерческую тайну, если она отвечает определенным требованиям.
2. Сведения, отвечающие законодательству РФ к коммерческой тайне.
3. Информация, являющаяся собственностью государственных структур.
4. Сведения, которые не могут быть отнесены к государственной тайне.

7. Что такое служебная тайна?

1. Служебная информация о деятельности государственных организаций.
2. Охраняемые государством сведения в любой области науки, техники, производства и управления, разглашение которых может нанести ущерб интересам государства.
3. Информация, которая не является государственной тайной.
4. Информация, которая не может быть отнесена к служебной тайне.

8. Что такое профессиональная тайна?

1. Защищаемая по закону информация, доверенная или ставшая известной лицу исключительно в Сулу исполнения им своих профессиональных обязанностей.
2. Если она отвечает охраноспособности права.
3. Информация, распространение которой может нанести ущерб правам доверителя.

4. Информация не являющаяся государственной или коммерческой тайной.

9.Что такое персональные данные?

1. Любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных).
2. Конфиденциальная информация, перечень которой закреплен Федеральным законом.
3. Биографические и опознавательные данные (в том числе об обстоятельствах рождения, усыновления, развода).
4. Сведения об имущественном, финансовом положении и о состоянии здоровья.

10. Что такое источники права на доступ к информации?

1. Наряду с Конституцией РФ источниками права о доступе к информации является: законы, подзаконные, нормативные акты, международные правовые акты, договоры и соглашения.
2. Государственные информационные ресурсы на доступ к которым не требуется обосновывать необходимость получения запрашиваемой информации.
3. Информация, полученная на законных основаниях из государственных информационных ресурсов.
4. Информационное обеспечения пользователей по вопросам прав, свобод и обязанностей граждан,

Тема 5. Основы криптографии

Вопросы:

1. Методы криптографии.
2. Симметричное и асимметричное шифрование. Алгоритмы шифрования.
3. Электронно-цифровая подпись. Алгоритмы электронно-цифровой подписи.
4. Криптографические генераторы случайных чисел. Способы распространения ключей.
5. Обеспечиваемая шифром степень защиты. Криптоанализ и атаки на криптосистемы.
6. Сжатие информации.

Рекомендации по изучению темы:

Вопрос 1,6 темы следует изучить по учебнику 2 основной литературы.
Вопрос 2,5 изложен в учебнике 2 дополнительной литературы.
Для самостоятельного изучения вопроса 3,4 следует обратиться к учебнику 1 основной литературы.

Контрольные вопросы:

1. Криптографические методы информационной безопасности.
2. Классификация методов криптографического закрытия информации.
3. Чем занимается наука криптология?
4. Что такое криптоанализ?
5. Стойкость криптографического метода это.
6. Основные требования к криптографическому закрытию информации?.
7. Шифрование это.
8. Классификация криптосистем.
9. Симметричные криптосистемы.
10. Классификация симметричных криптосистем.

11. Шифрование методом замены (подстановки).
12. Одноалфавитная подстановка.
13. Многоалфавитная одноконтурная обыкновенная подстановка.
14. Многоалфавитная одноконтурная монофоническая подстановка.
15. Многоалфавитная многоконтурная подстановка.
16. Шифрование методом перестановки.
17. Шифрование методом гаммирования.
18. Шифрование с помощью аналитических преобразований.
19. Комбинированные методы шифрования.
20. Криптосистемы с открытым ключом (асимметричные).
21. Характеристики существующих шифров.
22. Кодирование это
23. Стеганография это
24. Основные правила криптозащиты.
25. Основные правилами механизма распределения ключей.
26. Электронная цифровая подпись.
27. Технология электронной цифровой подписи.
28. Владелец сертификата ключа подписи это.
29. Средства электронной цифровой подписи это.
30. Сертификат средств электронной цифровой подписи это.
31. Закрытый ключ электронной цифровой подписи это.
32. Открытый ключ электронной цифровой подписи это.
33. Сертификат ключа подписи это.

Ответьте на тестовые вопросы:

11. Информация, к которой нельзя ограничивать доступ? (несколько вариантов):

1. Информация о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну.
2. Информация о состоянии окружающей среды.
3. Коммерческая тайна.
4. Банковская тайна.

12. Что такое информация с ограниченным доступом?

1. Информация, доступ к которой ограничен федеральными законами
2. Закон о коммерческой тайне.
3. Информация, полученная на законных основаниях из государственных информационных ресурсов.
4. Сведения об имущественном, финансовом положении и о состоянии здоровья.

13. Что такое надежность информации?

1. Под надежностью информации понимается интегральный показатель, характеризующий ее целостность, отсутствие в ней подмены.
2. Комплекс мер по защите информации в ходе непрерывного процесса подготовки,
обработки, хранения и передачи информации.
3. Безопасность информации.
4. Уверенность в том, что преданные владельцем данные не будут

размножаться, копироваться и использоваться без его санкции.

14. В чем заключается уязвимость информации?
1. заключается в нарушении ее физической сохранности, структурной целостности, доступности для правомочных пользователей..
2. Современные АС могут быть объектом случайных и умышленных воздействий.
3. Вероятность нарушения защищаемых характеристик АС.
4. В наличие и количестве дестабилизирующих факторов, потенциально возможных в структурных компонентов автоматизированных систем.

15. Сложность обеспечения информационной безопасности является следствием:
1. злого умысла разработчиков информационных систем
2. объективных проблем современной технологии программирования
3. происков западных спецслужб, встраивающих "закладки" в аппаратуру и программы

16. В число универсальных сервисов безопасности входят:
1. "разделяй и властвуй"
2. разделение обязанностей
3. инкапсуляция наследования
4. Метод «запрос-»

17. Комплексное экранирование может обеспечить (несколько вариантов):
1. разграничение доступа по сетевым адресам
2. выборочное выполнение команд прикладного протокола
3. контроль объема данных, переданных по TCP-соединению

18. Перехват данных является угрозой:
1. доступности
2. конфиденциальности
3. целостности
4. защиты от копирования

19. Что из перечисленного не относится к числу основных аспектов информационной безопасности:
1. доступность
2. целостность
3. защита от копирования
4. конфиденциальность

20. В число целей политики безопасности верхнего уровня входят (несколько вариантов):
1. формулировка административных решений по важнейшим аспектам
2. реализации программы безопасности
3. выбор методов аутентификации пользователей
4. обеспечение базы для соблюдения законов и правил

Тема 6. Антивирусные средства защиты
Вопросы:

1. Понятие и классификация вирусов.
2. Антивирусное программное обеспечение.

Рекомендации по изучению темы:
Вопрос 1 темы следует изучить по учебнику 1 основной литературы.
Вопрос 2, изложен в учебнике 1 дополнительной литературы.

Контрольные вопросы:

1. Признаки заражения компьютера.
2. Косвенные признаки заражения компьютера.
3. Действия при появлении признаков заражения вредоносной программой.
4. Источники компьютерных вирусов.
5. Глобальные сети и электронная почта как источник компьютерных вирусов.
6. Локальные сети как источник компьютерных вирусов.
7. Основные правила защиты от компьютерных вирусов.
8. Антивирусные программы.
9. Виды антивирусных программ.
10. Типовой перечень функций, которые способны выполнять антивирусные программы.

Ответьте на тестовые вопросы:
21. В число граней, позволяющих структурировать средства достижения информационной безопасности, входят:
1. законодательные меры
2. меры обеспечения доступности
3. профилактические меры
4. совокупность целей безопасности

22. В число этапов управления рисками входят (несколько вариантов):
1. анализ угроз
2. угрозы проведения анализа
3. выявление уязвимых мест

23. Агрессивное потребление ресурсов является угрозой:
1. доступности
2. конфиденциальности
3. целостности
4. защиты от копирования

24. В рамках программы безопасности нижнего уровня определяются:
1. совокупность целей безопасности
2. набор используемых механизмов безопасности
3. наиболее вероятные угрозы безопасности
4. совокупность целей безопасности

25. Что из перечисленного относится к числу основных аспектов

информационной безопасности:

1. подотчетность - полнота регистрационной информации о действиях субъектов
2. приватность - сокрытие информации о личности пользователя
3. конфиденциальность - защита от несанкционированного ознакомления

26. На современном этапе развития законодательного уровня информационной безопасности в России важнейшее значение имеют:

1. меры ограничительной направленности
2. направляющие и координирующие меры
3. меры по обеспечению информационной независимости

совокупность целей безопасности

Тема 7. Основные технологии построения защищенных экономических информационных систем

Вопросы:

1. Какие существуют виды стандартов и спецификаций?
2. Что такое «оценочные стандарты»?
3. Рассказать об «Оранжевой книге».
4. Что такое «доверенная вычислительная база»?
5. Что такое «периметр безопасности»?
6. Рассказать об уровнях доверия для вычислительных систем.
7. Рассказать о классах безопасности.
8. Рассказать о технической спецификации X.800.
9. Рассказать о сетевых механизмах безопасности.

Рекомендации по изучению темы:

Вопрос 1,3,5,7 темы следует изучить по учебнику 1 и 2 основной литературы.
Вопрос 2,4, изложен в учебнике 1 дополнительной литературы.
Для самостоятельного изучения вопроса 6,8 следует обратиться к учебнику 1 дополнительной литературы.

Контрольные вопросы:

1. Контроль и ревизия операций с денежными средствами и ценными бумагами
2. Контроль и ревизия операций с товарно-материальными ценностями.
3. Контроль и ревизия операций с основными средствами и не- материальными активами.
4. Контроль и ревизия долгосрочных инвестиций во внеоборотные активы.
5. Контроль и ревизия использования трудовых ресурсов и расчетов по оплате труда.

Ответьте на тестовые вопросы:

Основными компонентами парольной системы являются (несколько вариантов):

1. интерфейс администратора
2. хранимая копия пароля
3. база данных учетных записей
4. все варианты верны

2. Некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации это ….

1. идентификатор пользователя
2. пароль пользователя
3. учетная запись пользователя
4. парольная система

3. К принципам информационной безопасности относятся (несколько вариантов):

1. скрытость
2. масштабность
3. системность
4. законность
5. открытости алгоритмов

4. Охрана персональных данных, государственной служебной и других видов информации ограниченного доступа это…

1. Защита информации
2. Компьютерная безопасность
3. Защищенность информации
4. Безопасность данных

5. Система физической безопасности включает в себя следующие подсистемы (несколько вариантов):

1. оценка обстановки
2. скрытность
3. строительные препятствия
4. аварийная и пожарная сигнализация

6. Какие степени сложности устройства Вам известны (несколько вариантов):

1. упрощенные
2. простые
3. сложные
4. оптические
5. встроенные

7. Какие компоненты входят в комплекс защиты охраняемых объектов (несколько вариантов):

1. сигнализация
2. охрана
3. датчики
4. телевизионная система

8. К выполняемой функции защиты относится:

1. внешняя защита
2. внутренняя защита
3. все варианты верны

9. Набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных:

1. Защита информации
2. Компьютерная безопасность
3. Защищенность информации
4. Безопасность данных

10. Средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрещения доступа к ним это:

1. информационная война
2. информационное оружие
3. информационное превосходство

Тема 8. Алгоритмы безопасности в компьютерных сетях

Вопросы:

1. Межсетевые экраны.
2. Проектирование МЭ.
3. Снифферы. Эксплоиты.
4. Атаки на сервера.
5. Атаки на рабочие станции.
6. Атака типа «отказ в обслуживании».
7. Протоколирование.
8. Сетевые защищенные протоколы.

Рекомендации по изучению темы:

Вопрос 1,3,5,7 темы следует изучить по учебнику 1 и 2 основной литературы.
Вопрос 2,4,6,8 изложен в учебнике 1 дополнительной литературы.

Контрольные вопросы:

1. Дать понятие сетевой угрозы и сетевой атаки.
2. Рассказать о категориях сетевых атак.
3. Дать краткую характеристику каждой из них.
4. Что такое атаки доступа. Понятия snooping, eavesdropping, interception.
5. Рассказать об атаке доступа warchalking.
6. Рассказать об атаках модификации.
7. Понятия замена, добавление, удаление.
8. Верно ли, что легче выполнить перехват, чем прослушивание?
9. Как называется атака в виде попытки вставить запись в бухгалтерскую книгу.
10. Что такое атака на отказ в обслуживании?
11. Виды DoS-атак.
12. Атаки на отказ от обязательств. Вид атаки «маскарад».
13. Что такое межсетевой экран?
14. Каковы различные архитектурные решения защиты локальной сети с использованием межсетевых экранов?
15. Перечислить популярные программные брандмауэры и дать их

характеристики.

16. Как производится настройка правил доступа в сеть для всех приложений и для индивидуального приложения?
17. Как просмотреть список приложений и какие группы приложений существуют?

Ответьте на тестовые вопросы:

11. Информация позволяющая ее обладателю при существующих или возможных обстоятельствах увеличивать доходы, сохранить положение на рынке товаров, работ или услуг это:

1. государственная тайна
2. коммерческая тайна
3. банковская тайна
4. конфиденциальная информация

12. Гарантия того, что при хранении или передаче информации не было произведено несанкционированных изменений:

1. конфиденциальность
2. целостность
3. доступность
4. аутентичность
5. аппелеруемость

13. Гарантия точного и полного выполнения команд в ИС:

1. надежность
2. точность
3. контролируемость
4. устойчивость
5. доступность

14. Уровень защиты, при котором затраты, риск, размер возможного ущерба были бы приемлемыми:

1. принцип системности
2. принцип комплексности
3. принцип непрерывности
4. принцип разумной достаточности
5. принцип гибкости системы

15. Совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты АС от заданного множества угроз безопасности:

1. Комплексное обеспечение информационной безопасности
2. Безопасность АС
3. Угроза информационной безопасности
4. атака на автоматизированную систему
5. политика безопасности

16. Особенностями информационного оружия являются (несколько вариантов):

1. системность
2. открытость
3. универсальность
4. скрытность

17. К функциям информационной безопасности относятся (несколько вариантов):
1. совершенствование законодательства РФ в сфере обеспечения информационной безопасности
2. выявление источников внутренних и внешних угроз
3. страхование информационных ресурсов
4. защита государственных информационных ресурсов
5. подготовка специалистов по обеспечению информационной безопасности

18. К типам угроз безопасности парольных систем относятся
1. словарная атака
2. тотальный перебор
3. атака на основе психологии
4. разглашение параметров учетной записи
5. все варианты ответа верны

19. Хранение паролей может осуществляться (несколько вариантов):
1. в открытом виде
2. в закрытом виде
3. в зашифрованном виде
4. все варианты ответа верны

20. Антивирусная программа принцип работы, которой основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых вирусов называется:
1. ревизором
2. иммунизатором
3. сканером
4. доктора и фаги

21. Выбрать недостатки имеющиеся у антивирусной программы ревизор (несколько вариантов):
1. неспособность поймать вирус в момент его появления в системе
2. небольшая скорость поиска вирусов
3. невозможность определить вирус в новых файлах (в электронной почте, на дискете)

22. В соответствии с особенностями алгоритма вирусы можно разделить на два класса (несколько вариантов):
1. вирусы изменяющие среду обитания, но не распространяющиеся
2. вирусы изменяющие среду обитания при распространении
3. вирусы не изменяющие среду обитания при распространении
4. вирусы не изменяющие среду обитания и не способные к распространению в дальнейшем

23. К достоинствам технических средств защиты относятся:

1. регулярный контроль
2. создание комплексных систем защиты
3. степень сложности устройства
4. Все варианты верны

24. К тщательно контролируемым зонам относятся (несколько вариантов):

1. рабочее место администратора
2. архив
3. рабочее место пользователя
4. учетная запись пользователя
5. парольная система

25. К системам оповещения относятся (несколько вариантов):

1. инфракрасные датчики
2. электрические датчики
3. электромеханические датчики
4. электрохимические датчики

26. К оборонительным системам защиты относятся (несколько вариантов):

1. проволочные ограждения
2. звуковые установки
3. датчики
4. световые установки

27. Охранное освещение бывает (несколько вариантов):

1. дежурное
2. световое
3. Тревожное