Министерство науки и высшего образования РФ
ФГБОУ ВО «Ульяновский государственный университет»
Институт экономики и бизнеса

Сковиков А.Г.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ПО ДИСЦИПЛИНЕ «ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ»

для магистрантов направления 38.04.01 «Экономика» (профиль «Экономическая безопасность организации») всех форм обучения

Ульяновск, 2019

Методические указания для самостоятельной работы студентов по дисциплине «Обеспечение информационной безопасности организации» / составитель: А.Г. Сковиков. - Ульяновск: УлГУ, 2019.

Настоящие методические указания предназначены для студентов магистратуры по направлению 38.04.01 «Экономика» (профиль «Экономическая безопасность организации») всех форм обучения, изучающих дисциплину «Обеспечение информационной безопасности организации».

В работе приведены литература по дисциплине, основные темы курса и вопросы в рамках каждой темы, рекомендации по изучению теоретического материала, контрольные вопросы для самоконтроля, кейсы и тесты для самостоятельной работы.

Студентам заочной формы обучения следует использовать данные методические указания при самостоятельном изучении дисциплины, при подготовке к практическим занятиям и к промежуточной аттестации по данной дисциплине.

Рекомендованы к введению в образовательный процесс Ученым советом Института экономики и бизнеса УлГУ (протокол № 223/09 от 27 июня 2019 г.).

1. ЛИТЕРАТУРА ДЛЯ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

1. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для академического бакалавриата / И. Н. Васильева. — Москва : Издательство Юрайт, 2018. — 349 с. — (Бакалавр. Академический курс). — ISBN 978-5-534-02883-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://www.biblio-online.ru/bcode/413761 .

2. Внуков, А. А. Защита информации в банковских системах : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2018. — 246 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-01679-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://www.biblio-online.ru/bcode/414083

3. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для академического бакалавриата / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2018. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://www.biblio-online.ru/bcode/422364

4. Бирюков А.А., Информационная безопасность: защита и нападение / Бирюков А. А. - М. : ДМК Пресс, 2017. - 434 с. - ISBN 978-5-97060-435-9 - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : http://www.studentlibrary.ru/book/ISBN9785970604359.html

5. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2017. — 312 с. — (Специалист). — ISBN 978-5-9916-9043-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://www.biblio-online.ru/bcode/395848

6. Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — Москва : Издательство Юрайт, 2018. — 321 с. — (Университеты России). — ISBN 978-5-534-00258-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://www.biblio-online.ru/bcode/414248

7. 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, 2018. — 325 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://www.biblio-online.ru/bcode/413158

8. Чекмарев, А. В. Управление ит-проектами и процессами : учебное пособие для

академического бакалавриата / А. В. Чекмарев. — Москва : Издательство Юрайт, 2018. — 228 с. — (Бакалавр. Академический курс). — ISBN 978-5-534-07446-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://www.biblio-online.ru/bcode/423098

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ

ТЕМА 1. ОСНОВНЫЕ ПОНЯТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ЖИЗНЕННЫЙ ЦИКЛ КОНТЕНТА. ПЛАТФОРМЫ ДЛЯ ЭФФЕКТИВНОЙ КОРПОРАТИВНОЙ РАБОТЫ.

Основные вопросы:

1. Современная концепция информационной безопасности. Цели защиты информации. Носители защищаемой информации. Понятие информации. Сведения и данные, отличие от информации. Информация по уровню доступа. Конфиденциальность информации. Понятие конфиденциальной информации. Классификация конфиденциальной информации. Понятие государственной тайны.

2. Понятие угроз безопасности. Классификация угроз информационной безопасности. Основная классификация угроз: угрозы нарушения конфиденциальности информации, угрозы нарушения целостности информации, угрозы нарушения доступности информации. Методы перечисления угроз. Случайные и преднамеренные угрозы.

Рекомендации по изучению темы:

Вопрос 1 рассмотрен в учебнике [5] на с. 12-14, учебнике [6] на с. 10-15, учебнике [7] на с. 10-16; 157-204.

Вопрос 2 рассмотрен в учебнике [2] на с. 48-50, учебнике [5] на с. 14-24.

Контрольные вопросы:

1. Дайте определение понятию информационная безопасность.
2. Охарактеризуйте основные составляющие национальных интересов РФ в информационной сфере.
3. Охарактеризуйте угрозы информационной безопасности РФ.
4. Охарактеризуйте комплекс мер по совершенствованию информационной безопасности РФ.
5. Дайте понятие метода обеспечения информационной безопасности.
6. Что понимается под жизненно важными интересами личности, общества и государства в информационной сфере?
7. Как соотносятся понятия "информационная безопасность", "безопасность информации" и "защита информации"?

8. Каковы согласно Доктрине информационной безопасности Российской Федерации основные составляющие национальных интересов Российской Федерации в информационной сфере?

9. Сформулируйте основные задачи в области обеспечения информационной безопасности.

10. Перечислите уровни решения проблемы информационной безопасности.

11. Перечислите уровни защиты информации.

12. Охарактеризуйте угрозы информационной безопасности: раскрытия целостности, отказ в обслуживании.

13. Объясните причины компьютерных преступлений.

14. Опишите, как обнаружить компьютерное преступление или уязвимые места в системе информационной безопасности.

15. Опишите основные технологии компьютерных преступлений.

16. Перечислите меры защиты информационной безопасности.

Кейсы для самостоятельной работы:

1. Проанализируйте состояние информационной безопасности в Вашем учебном заведении. Предложите дополнительные мероприятия по повышению уровня информационной безопасности.

2. Приведите примеры из жизни, из кино- и видеофильмов, иллюстрирующие использование уязвимых мест и нарушения мер защиты информационной безопасности для несанкционированного проникновения в охраняемые системы.

3. Проведите анализ использования носителей в компьютерном классе Вашего учебного заведения с точки зрения обеспечения норм информационной безопасности, сформулируйте предложения по укреплению информационной безопасности кабинета.

Тесты для самостоятельной работы:

1. Информационная безопасность
   a) сводится исключительно к защите от несанкционированного доступа к информации
   b) является аналогом определения "компьютерная безопасность"
   c) это состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства
   d) понимается как состояние защищенности от всех возможных видов ущерба

2. В состав поддерживающей инфраструктуры входят:
   a) электро-, водо- и теплоснабжение
   b) обслуживающий персонал
   c) компьютеры
   d) кондиционеры
   e) средства коммуникаций

3. Направления защиты государственной тайны:
   a) Обеспечение режима секретности
   b) Криптографическая защита
   c) Противодействие техническим средствам разведки
   d) Защита ЭВМ, баз данных и компьютерных систем
   e) Противодействие информационному оружию

4. Направления защиты конфиденциальной информации общественного назначения:
   a) Обеспечение режима секретности
   b) Криптографическая защита
   c) Противодействие техническим средствам разведки
   d) Защита ЭВМ, баз данных и компьютерных систем
   e) Противодействие информационному оружию

5. Направления защиты конфиденциальной информации личности:
   a) Обеспечение режима секретности
   b) Криптографическая защита
   c) Противодействие техническим средствам разведки
   d) Защита ЭВМ, баз данных и компьютерных систем
   e) Противодействие информационному оружию

   a) Основные составляющие информационной безопасности информационных ресурсов и поддерживающей инфраструктуры:
   b) обеспечение доступности
   c) обеспечение целостности
   d) обеспечение конфиденциальности
   e) обеспечение оптимального уровня затрат
   f) обеспечение требований стандартов безопасности

6. Возможность за приемлемое время получить требуемую информационную услугу - это
   a) доступность
   b) целостность
   c) конфиденциальность
   d) работоспособность
   e) мощность

7. Защищенность информации от разрушения и несанкционированного изменения - это
   a) доступность
   b) целостность
   c) конфиденциальность
   d) работоспособность
   e) актуальность

8. Важнейшим элементом информационной безопасности является
   a) доступность
   b) целостность
   c) конфиденциальность
   d) аутентичность

9. Самыми частыми и самыми опасными (с точки зрения размера ущерба) угрозами доступности являются

a) непреднамеренные ошибки штатных пользователей, операторов, системных администраторов
b) пожары и наводнения
c) внутренние отказы информационной системы
d) отказы поддерживающей инфраструктуры
e) действия злоумышленников

10. Основными источниками внутренних отказов являются:
a) отступление (случайное или умышленное) от установленных правил эксплуатации
b) невозможность работать с системой в силу отсутствия соответствующей подготовки
c) разрушение или повреждение аппаратуры
d) разрушение данных
e) отказы программного и аппаратного обеспечения

11. Основными источниками отказов пользователей являются:
a) нежелание работать с информационной системой
b) невозможность работать с системой в силу отсутствия соответствующей подготовки
c) разрушение данных
d) отказы программного и аппаратного обеспечения
e) отступление (случайное или умышленное) от установленных правил эксплуатации

12. Примерами угроз доступности являются:
a) протечки водопровода и отопительной системы
b) поломка кондиционеров, установленные в серверных залах
c) агрессивное потребление ресурсов (полосы пропускания сетей, вычислительных возможностей процессоров или оперативной памяти)
d) нарушение атомарности транзакций
e) методы морально-психологического воздействия, такие как маскарад

13. Кто является основным ответственным за определение уровня классификации информации?
a) Руководитель среднего звена
b) Высшее руководство
c) Владелец
d) Пользователь

14. Что самое главное должно продумать руководство при классификации данных?
a) Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
b) Необходимый уровень доступности, целостности и конфиденциальности
c) Оценить уровень риска и отменить контрмеры
d) Управление доступом, которое должно защищать данные

ТЕМА 2. РИСКИ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ.

Основные вопросы темы:

1. Оценка рисков: выбор анализируемых объектов и уровня детализации их рассмотрения; выбор методологии оценки рисков; идентификация активов; анализ угроз и их последствий, выявление уязвимых мест в защите; оценка рисков; выбор защитных мер; реализация и проверка выбранных мер; оценка остаточного риска.

Рекомендации по изучению темы:

Вопрос 1 рассмотрен в учебнике [6] на с. 121-192, учебнике [7] на с. 40-114.

Контрольные вопросы:

1. Что должна определять модель данных?
2. Перечислите и охарактеризуйте три уровня моделей базы данных.
3. Каковы основные модели данных?
4. Какие основные структуры данных определены в иерархической модели данных?
5. Какие операции предусматриваются иерархической моделью данных?
6. Чем в сетевой модели данных агрегат типа «вектор» отличается от агрегата типа «повторяющаяся группа»?
7. В чем особенности набора в сетевой модели данных по сравнению с групповым отношением в иерархической модели?
8. Какие типы членства записи в наборе допускает сетевая модель?
9. Перечислите операции, определенные в сетевой модели данных, сравните их с операциями иерархической модели.

Кейсы для самостоятельной работы:

1. Проведите анализ понятийного аппарата и необходимости раскрытия понятий «информационное оружие», «информационные войны». Изучите Таллинские рекомендации, в чем их уязвимые места? Какие понятия используются в России и в США в этой сфере: «кибербезопасность» или «информационная безопасность»? Обоснуйте позицию России.

Тесты для самостоятельной работы:

1. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?
   a) Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
   b) Когда риски не могут быть приняты во внимание по политическим соображениям
   c) Когда необходимые защитные меры слишком сложны
   d) Когда стоимость контрмер превышает ценность актива и потенциальные потери

2. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?
   a) Анализ рисков
   b) Анализ затрат / выгоды
   c) Результаты ALE
   d) Выявление уязвимостей и угроз, являющихся причиной риска

3. Как рассчитать остаточный риск?
   a) Угрозы х Риски х Ценность актива
   b) (Угрозы х Ценность актива х Уязвимости) х Риски
   c) SLE х Частоту = ALE
   d) (Угрозы х Уязвимости х Ценность актива) х Недостаток контроля

4. Что из перечисленного не является целью проведения анализа рисков?
   a) Делегирование полномочий
   b) Количественная оценка воздействия потенциальных угроз
   c) Выявление рисков
   d) Определение баланса между воздействием риска и стоимостью необходимых контрмер

5. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?
   a) Чтобы убедиться, что проводится справедливая оценка
   b) Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ
   c) Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа
   d) Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку

6. Что является наилучшим описанием количественного анализа рисков?
   a) Анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности
   b) Метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков
   c) Метод, сопоставляющий денежное значение с каждым компонентом оценки рисков
   d) Метод, основанный на суждениях и интуиции

7. Почему количественный анализ рисков в чистом виде не достижим?
   a) Он достижим и используется
   b) Он присваивает уровни критичности. Их сложно перевести в денежный вид.
   c) Это связано с точностью количественных элементов
   d) Количественные измерения должны применяться к качественным элементам

8. Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется так много времени для проведения анализа?
   a) Много информации нужно собрать и ввести в программу
   b) Руководство должно одобрить создание группы
   c) Анализ рисков не может быть автоматизирован, что связано с самой природой оценки
   d) Множество людей должно одобрить данные

9. Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой?
   a) Анализ связующего дерева
   b) AS/NZS
   c) NIST
   d) Анализ сбоев и дефектов

10. В Законе "Об информации" определение "обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя" относится к понятию
   a) доступ к информации
   b) конфиденциальность информации

c) предоставление информации
d) распространение информации

11. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?
a) Поддержка высшего руководства
b) Эффективные защитные меры и методы их внедрения
c) Актуальные и адекватные политики и процедуры безопасности
d) Проведение тренингов по безопасности для всех сотрудников

a) Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?
b) Только военные имеют настоящую безопасность
c) Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности
d) Военным требуется больший уровень безопасности, т.к. их риски существенно выше
e) Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности

12. Защита информации от утечки - это деятельность по предотвращению:
a) получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
b) 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;
c) воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
d) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
e) несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

13. Защита информации это:
a) процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
b) преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
c) получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
d) совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
e) деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

ТЕМА 3. ITIL/ITSM − КОНЦЕПТУАЛЬНАЯ ОСНОВА ПРОЦЕССОВ IT –СЛУЖБЫ. РЕШЕНИЯ HEWLETT-PACKARD ПО УПРАВЛЕНИЮ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ. РЕШЕНИЯ IBM ПО УПРАВЛЕНИЮ ИНФОР-МАЦИОННЫМИ СИСТЕМАМИ.

Основные вопросы темы:

1. Общие сведения о библиотеке ITIL. Модель ITSM.
2. Соглашение об уровне сервиса.
3. Модель информационных процессов ITSM Reference Model.

Рекомендации по изучению темы:

Вопрос 1 рассмотрен в учебнике [8] на с. 189-207.

Вопрос 1 рассмотрен в учебнике [8] на с. 207-210.

Контрольные вопросы:

2. Чем модель ITSM отличается от традиционного функционального подхода к организации ИТ-службы?
3. Перечислите особенности проекта ITIL?
4. Какие разделы управления ИТ-сервисами описаны в текущей версии биб-лиотеки ITIL?
5. Какие направления управления ИТ-услугами описаны в проекте ITIL Refresh?
6. Какие процессы включены в блок поддержки ИТ-сервисов?
7. Какие процессы включены в блок предоставления ИТ-сервисов?
8. Поясните назначение процесса управления инцидентами.
9. Поясните понятие "инцидент".
10. Приведите основные функции процесса управления инцидентами.
11. Поясните назначение процесса управления проблемами. 27. Поясните понятие "проблема".
12. Приведите основные функции процесса управления проблемами.
13. Поясните назначение процесса управления конфигурациями.
14. Поясните понятие "конфигурационная единица".
15. Для чего используется база данных конфигурационных единиц– CMDB?
16. Что могут описывать атрибуты конфигурационных единицах в CMDB?
17. Какие важные понятия описываются в спецификации процесса управления конфигурациями?
18. Поясните назначение процесса управления изменениями.
19. Приведите основные функции процесса управления изменениями.
20. Поясните назначение процесса управления релизами.

21. Поясните понятие "релиз".

22. Как классифицируются релизы по показателю масштаба изменений?

23. Приведите основные функции процесса управления релизами.

24. Поясните назначение библиотеки эталонного ПО - DSL.

25. Поясните назначение процесса управления уровнем сервиса.

26. Поясните понятие "соглашение об уровне сервиса - SLA".

27. Приведите основные функции процесса управления уровнем сервиса.

28. Поясните назначение процесса управления мощностями.

29. Приведите основные функции процесса управления мощностями.

30. Поясните назначение процесса управления доступностью.

31. Поясните понятие "доступностью ИТ-сервиса".

32. Приведите основные функции процесса управления доступностью.

33. Поясните назначение процесса управления непрерывностью.

34. Приведите основные функции процесса управления непрерывностью.

35. Поясните назначение процесса управления финансами ИТ-службы.

36. Приведите основные функции процесса управления финансами ИТ-службы.

37. Поясните назначение процесса управления безопасностью.

38. Поясните возможность применения модели ITSM на предприятиях различного размера.

39. Поясните сущность реактивного принципа работы службы ИТ-поддержки

40. Поясните сущность проактивного принципа работы службы ИТ-поддержки.

41. Поясните основное назначение блока процессов "Согласование задач бизнеса и ИТ".

42. Поясните основное назначение блока процессов "Планирование и управление ИТсервисами".

43. Поясните основное назначение блока процессов "Разработка и внедрение ИТ-сервисов".

44. Поясните основное назначение блока процессов "Оперативное управление ИТ - сервисами".

45. Поясните основное назначение блока процессов "Обеспечение ИТ-сервисами".

46. Назовите основные стадии внедрения процессного управления ИТ-службы предприятия.

47. Какие процессы внедряются на стадии "Управление ИТ-инфраструктурой"?

48. Какие процессы внедряются на стадии "Управление сервисами"?

49. Какие процессы внедряются на стадии "Управление деловыми характеристиками ИТ"?

50. Как соотносятся модель ITPM (IT ProcessModel) и библиотека ITIL?

51. Какие группы процессов определены в ITPM?

52. Поясните сущность процесса "Улучшение взаимодействия с клиентами"?

53. Поясните сущность процесса "Обеспечение управленческих систем корпоративной информацией".

54. Поясните сущность процесса "Управление ИТ-инфраструктурой с точки зрения бизнеса".

55. Поясните сущность процесса "Реализация и развертывание решений".

56. Поясните сущность процесса "Обеспечение ИТ-сервисами".

57. Поясните сущность процесса "Поддержка ИТ-сервисов и решений".

58. Поясните сущность процесса "Управление ИТ-ресурсами и ИТ-инфраструктурой".

59. В каком году опубликован первый вариант типовой модели HP ITSM - ITSM Reference Model?

60. Какие основные группы процессов определены в методологии HP — ITSM Reference Model?

61. Поясните основное назначение блока процессов «Согласование задач бизнеса и ИТ».

62. Поясните основное назначение блока процессов «Планирова-ние и управление ИТ-сервисами».

63. Поясните основное назначение блока процессов «Разработка и внедрение ИТ-сервисов».

64. Поясните основное назначение блока процессов «Оперативное управление ИТ-сервисами».

65. Поясните основное назначение блока процессов «Обеспечение ИТ-сервисами».

66. Назовите основные стадии внедрения процессного управления ИТ-службы предприятия.

67. Какие процессы внедряются на стадии «Управление ИТ-инфраструктурой»?

68. Какие процессы внедряются на стадии «Управление сервиса-ми»?

69. Какие процессы внедряются на стадии «Управление деловыми характеристиками ИТ»?

70. Назовите набор основных решений HP OpenView, предназна-ченных для централизованного управления ИТ-ресурсами предприятия.

71. Охарактеризуйте решение HP OpenView «Управление бизне-сом».

72. Охарактеризуйте решение HP OpenView «Управление прило-жениями».

73. Охарактеризуйте решение HP OpenView «Управление ИТ-инфраструктурой».

74. Охарактеризуйте решение HP OpenView «Управление ИТ-службой».

75. Охарактеризуйте решение HP OpenView «Управление иденти-фикацией».

76. Охарактеризуйте решение HP OpenView «Service Desk».

77. Охарактеризуйте решение HP OpenView «Network Node Manager».

78. Поясните назначение пакета программ HP OpenView Compliance Manager.

79. Поясните назначение пакета программ HP OpenView Performance Insight.

80. Поясните назначение пакета программ HP OpenView Reporter.

81. Поясните назначение пакета программ HP OpenView Dashboard.

82. Поясните назначение пакета программ HP OpenView Information Portal.

83. Поясните назначение пакета программ HP OpenView Business Process Insight.

84. Как соотносятся модель ITPM (IT Process Model) и библиотека ITIL?

85. Какие группы процессов определены в ITPM?

86. Поясните сущность процесса «Улучшение взаимодействия с клиентами»?

87. Поясните сущность процесса «Обеспечение управленческих систем корпоративной информацией».

88. Поясните сущность процесса «Управление ИТ-инфраструктурой с точки зрения бизнеса».

89. Поясните сущность процесса «Реализация и развертывание решений».

90. Поясните сущность процесса «Обеспечение ИТ-сервисами».

91. Поясните сущность процесса «Поддержка ИТ-сервисов и решений».

92. Поясните сущность процесса «Управление ИТ-ресурсами и ИТ-инфраструктурой».

93. Что позволяет реализовать программное обеспечение Tivoli в плане бизнес-ориентрованного управления ИТ-инфраструктурой предприятия?

94. Какие области управления ИТ-инфраструктурой предприятия включают специализированные решения платформы Tivoli?

95. Какие функции операционной поддержки Tivoli позволяют снизить потенциальный уровень затрат, автоматизировать управление и повысить его эффективность?

96. Какие решения IBM Tivoli поддерживают базовые технологии?

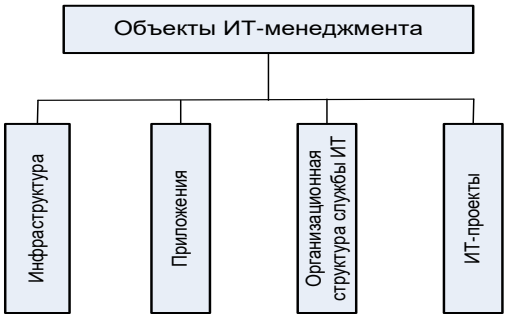
97. Поясните основные функции программного продукта Tivoli Enterprise Data Warehouse.

98. Поясните основные функции программного продукта Tivoli Management Framework.

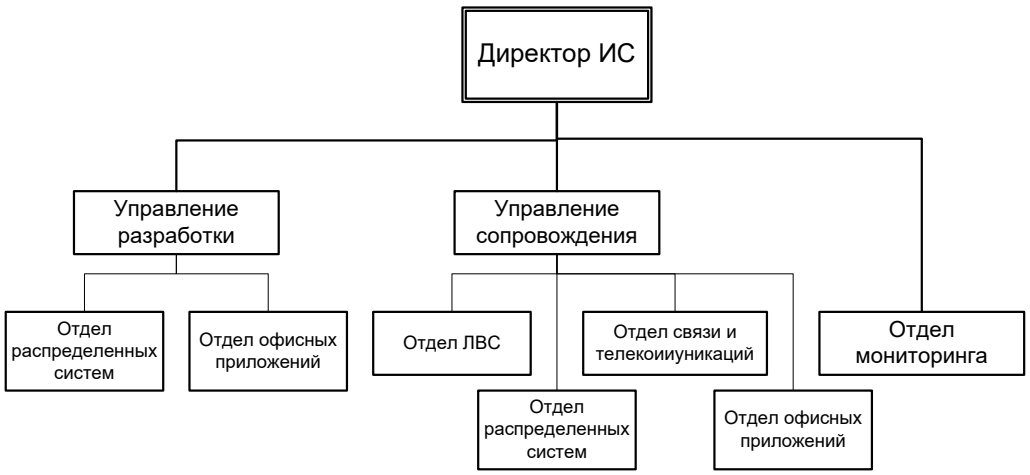
99. Поясните основные функции программного продукта Tivoli Universal Agent.

Кейсы для самостоятельной работы:

1. Прокомментируйте состав и содержание объектов информационного менеджмента



2. Прокомментируйте дублирование ИТ-подразделений в плоской структуре службы ИС



Тесты для самостоятельной работы:

1. Соглашение с внутренним ИТ-подразделением, конкретизирующим договоренности о предоставлении определенных элементов сервисов, называется:
   a) SLA
   b) ERP
   c) OLA
   d) UC
   e) ITSM

2. Какие процессы относятся к поддержке ИТ-сервисов:
   a) управление инцидентами
   b) управление проблемами
   c) управление конфигурациями
   d) управление изменениями
   e) управление релизами
   f) все ответы верны
   g) все ответы неверны.

3. Какие процессы относятся к предоставлению ИТ-сервисов:
   a) управление мощностью
   b) управление проблемами
   c) управление конфигурациями
   d) управление безопасностью
   e) управление уровнем сервиса
   f) управление доступностью
   g) все ответы верны
   h) все ответы неверны.

4. Какой процесс на основании каталога ИТ-сервисов разрабатывает, согласовывает и документирует SLA между менеджментом ИТ-службы и бизнес-пользователями?
   a) процесс управления безопасностью
   b) процесс управления мощностью
   c) процесс управления релизами
   d) процесс управления уровнем сервиса
   e) процесс управления непрерывностью.

5. Сколько и какие книги входят в ITIL третьей версии?
   a) 5 книг - Service Model, Service Design, Service Delivery, Service Transition, Service Operation
   b) 2 книги - Service Delivery, Service Support
   c) 7 книг - Service Strategy, Continual Service Improvement, Service Portfolio Management, Service Transition, Service Operation, IT Service Continuity Management, Service Knowledge Management System
   d) 3 книги - Service Delivery, Service Model, Service Support
   e) 5 книг - Service Strategy, Continual Service Improvement, Service Design, Service Transition, Service Operation.

6. На какой стадии реализуется процесс ITSM Reference Model планирование развития сервисов
   a) стадия управления сервисами
   b) стадия управление деловыми характеристиками ИТ
   c) стадия управление инфраструктурой

7. Какое решение HP OpenView обеспечивает связь информационных технологий
   a) управление бизнесом
   b) управление приложениями
   c) управление перекрестными функциями

8. Какие программные решения предназначены для централизованного управления ИТ-ресурсами предприятия?
   a) Microsoft Outlook
   b) IBM Rational Rose
   c) HP OpenView

9. Какие параметры можно отследить с помощью мониторинга уровней обслуживания ИТ-сервисов
   a) время отклика по транзакции
   b) эффективность использования приложений
   c) коэффициенты загрузки ресурсов информационной системы

10. Какое решение HP OpenView поддерживает переход ИТ-службы предприятия на процессную основу
   a) управление конфигурациями
   b) управление ИТ-службой
   c) управление идентификацией

11. С помощью какого программного решения HP OpenView управление ИТ-службой обеспечивается эффективное управление ИТ-сервисами в распределенных системах
   a) управление активами
   b) поддержка пользователей
   c) управление объединенными событиями и производительностью

ТЕМА 4. ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ IT-ИНФРАСТРУКТУРЫ ПРЕДПРИЯТИЯ. ТЕХНОЛОГИЯ MICROSOFT ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

Основные вопросы темы:

1. Уровни зрелости ИТ-инфраструктуры предприятия.

Рекомендации по изучению темы:

Вопрос 1 рассмотрен в учебнике [8] на с. 163-188.

Контрольные вопросы:

1. Какие уровни зрелости предприятий определены в модели CMM/CMMI ?
2. Как характеризуется начальный уровень зрелости предприятия по модели CMM/CMMI?
3. Как характеризуется повторяемый уровень зрелости предприятия по модели CMM/CMMI?
4. Как характеризуется определенный уровень зрелости предприятия по модели CMM/CMMI?
5. Как характеризуется управляемый уровень зрелости предприятия по модели CMM/CMMI?
6. Как характеризуется оптимизирующий уровень зрелости предприятия по модели CMM/CMMI?
7. Какие уровни зрелости ИТ-инфраструктуры предложены компанией Gartner?
8. Какие профили предприятий для оптимизации ИТ-инфраструктуры определены компанией IBM?
9. Как характеризуется профиль commodity в модели IBM?
10. Как характеризуется профиль utility в модели IBM?
11. Как характеризуется профиль partner в модели IBM?
12. Как характеризуется профиль enabler в модели IBM?

13. Какие уровни зрелости ИТ-инфраструктуры предприятия предложены компанией Microsoft?

14. Как характеризуется базовый уровень зрелости ИТ-инфраструктуры в модели Microsoft?

15. Как характеризуется стандартизированный уровень зрелости ИТ-инфраструктуры в модели Microsoft?

16. Как характеризуется рационализированный уровень зрелости ИТ-инфраструктуры в модели Microsoft?

17. Как характеризуется динамический уровень зрелости ИТ-инфраструктуры в модели Microsoft?

18. Какие документы и руководства входят в состав библиотеки документов Microsoft Operations Framework (MOF)?

19. На каких принципах основывается модель процессов эксплуатации и функции управления услугами MOF?

20. Какие категории квадрантов входят в модель процессов MOF?

21. Какие процессы описаны в квадранте «Изменения» модели MOF?

22. Какие процессы описаны в квадранте «Эксплуатация» модели MOF? Какие процессы описаны в квадранте «Поддержка» модели MOF?

23. На какие уровни разделены процессы в квадранте «Эксплуатация»?

24. Какие процессы описаны в квадранте «оптимизация» модели MOF?

25. Какие роли участников процесса эксплуатации ИС определены в модели групп эксплуатации MOF?

Кейсы для самостоятельной работы:

1. Вариант 1. Проведите анализ организационной зрелости организации по степени использования информации и IT в его бизнес-процессах для овощебазы

2. Вариант 2. Проведите анализ организационной зрелости организации по степени использования информации и IT в его бизнес-процессах для туристического агентства

3. Вариант 3. Проведите анализ организационной зрелости организации по степени использования информации и IT в его бизнес-процессах для парикмахерской

4. Вариант 4. Проведите анализ организационной зрелости организации по степени использования информации и IT в его бизнес-процессах для рекламного агентства 26

5. Вариант 5. Проведите анализ организационной зрелости организации по степени использования информации и IT в его бизнес-процессах для предприятия оптовой торговли

6. Вариант 6. Проведите анализ организационной зрелости организации по степени использования информации и IT в его бизнес-процессах для предприятий розничной торговли

7. Вариант 7. Проведите анализ организационной зрелости организации по степени использования информации и IT в его бизнес-процессах для управляющей компании ЖКХ

8. Вариант 8. Проведите анализ организационной зрелости организации по степени использования информации и IT в его бизнес-процессах для гостиницы

9. Вариант 9. Проведите анализ организационной зрелости организации по степени использования информации и IT в его бизнес-процессах для ресторана

10. Вариант 10. Проведите анализ организационной зрелости организации по степени использования информации и IT в его бизнес-процессах для ювелирного магазина

11. Вариант 11. Проведите анализ организационной зрелости организации по степени использования информации и IT в его бизнес-процессах для высшего учебного заведения

12. Вариант 12. Проведите анализ организационной зрелости организации по степени использования информации и IT в его бизнес-процессах для банка

13. Вариант 13. Проведите анализ организационной зрелости организации по степени использования информации и IT в его бизнес-процессах для кафе

14. Вариант 14. Проведите анализ организационной зрелости организации по степени использования информации и IT в его бизнес-процессах для полиграфического салона 27

15. Вариант 15. Проведите анализ организационной зрелости организации по степени использования информации и IT в его бизнес-процессах для логистического центра

16. Вариант 16. Проведите анализ организационной зрелости организации по степени использования информации и IT в его бизнес-процессах для государственного учреждения

17. Вариант 17. Проведите анализ организационной зрелости организации по степени использования информации и IT в его бизнес-процессах для инвестиционной компании

18. Вариант 18. Проведите анализ организационной зрелости организации по степени использования информации и IT в его бизнес-процессах для строительной компании

19. Вариант 19. Проведите анализ организационной зрелости организации по степени использования информации и IT в его бизнес-процессах для промышленного предприятия

20. Вариант 20. Проведите анализ организационной зрелости организации по степени использования информации и IT в его бизнес-процессах для риэлтерской компании

Тесты для самостоятельной работы:

1. Модель оценки уровня зрелости бизнес-процессов предприятия SW-CMM разработана
   a) для программных продуктов
   b) для системной инженерии
   c) для закупок
   d) для управления людскими ресурсами

2. Модель оценки уровня зрелости бизнес-процессов предприятия SE-CMM разработана
   a) для программных продуктов
   b) для системной инженерии
   c) для закупок
   d) для интеграции продуктов

3. Модель оценки уровня зрелости бизнес-процессов предприятия Acquisition CMM разработана
   a) для программных продуктов
   b) для системной инженерии
   c) для закупок
   d) для интеграции продуктов

4. Модель оценки уровня зрелости бизнес-процессов предприятия ICMM разработана
   a) для программных продуктов
   b) для системной инженерии
   c) для закупок
   d) для интеграции продуктов

5. Выберите из списка комплексную модель оценки уровня зрелости бизнес-процессов предприятия, объединяющую остальные
   a) CMMI
   b) CMM
   c) ICMM
   d) Acquisition CMM

6. В модели CMM/CMMI определены следующие уровни зрелости предприятий:
   a) начальный
   b) повторяемый
   c) определенный
   d) совершенный

7. В модели CMM/CMMI определены следующие уровни зрелости предприятий:
   a) определенный
   b) управляемый
   c) оптимизирующий
   d) обеспеченный

8. Сколько уровней зрелости предприятий определены в модели CMM/CMMI?
(вводить следует цифрой)

9. Какой уровень зрелости предприятий модели CMM/CMMI предполагает внедрение формальных процедур для выполнения основных элементов процесса разработки ПО. Результаты выполнения процесса соответствуют заданным требованиям и стандартам

a) Начальный уровень
b) Повторяемый уровень
c) Определенный уровень
d) Управляемый уровень
e) Оптимизирующий уровень

10. Какой уровень зрелости предприятий модели CMM/CMMI предполагает наиболее сильную зависимость результатов деятельности предприятия от личных качеств отдельных сотрудников

a) Начальный уровень
b) Повторяемый уровень
c) Определенный уровень
d) Управляемый уровень
e) Оптимизирующий уровень

11. Начиная с какого уровня зрелости предприятий модели CMM/CMMI все элементы процесса разработки ПО должны быть формализованы, стандартизованы и задокументированы?

a) Начальный уровень
b) Повторяемый уровень
c) Определенный уровень
d) Управляемый уровень
e) Оптимизирующий уровень

12. Начиная с какого уровня зрелости предприятий модели CMM/CMMI все элементы процесса разработки ПО планируются и управляются на основе единого стандарта предприятия?

a) Начальный уровень
b) Повторяемый уровень
c) Определенный уровень
d) Управляемый уровень
e) Оптимизирующий уровень

13. В чем состоит основное отличие Управляемого уровня зрелости предприятий модели CMM/CMMI от Определенного уровня той же модели?

a) в более объективной, количественной оценке продукта и процесса разработки ПО
b) в том, что технология создания и сопровождения программных продуктов планомерно и последовательно совершенствуется
c) в том, что элементы процесса Управляемого уровня планируются и управляются на основе единого стандарта предприятия
d) в том, что выполнение процесса разработки ПО планируется и контролируется

14. Сколько уровней для оценки зрелости ИТ-службы предлагает использовать компания Gartner?
(вводить следует цифрой)

15. Компания Gartner предлагает для оценки зрелости ИТ-службы использовать следующие уровни

a) хаотичный

b) реактивный
c) сервис
d) оптимальный
e) развернутый

16. Компания Gartner предлагает для оценки зрелости ИТ-службы использовать следующие уровни проактивный
a) польза
b) сервис
c) реактивный
d) система

17. Какой уровень зрелости ИТ-инфраструктуры согласно классификции компании Gartner характеризуется тем, что на предприятии проводится отслеживание событий, имеется единая консоль и служба поддержки, осуществляется управление топологией сети, выполняется резервное копирование и инвентаризация?
a) хаотичный
b) реактивный
c) система
d) польза
e) проактивный

a) Начиная с какого уровня зрелости ИТ-инфраструктуры согласно классификции компании Gartner должно реализовываться управление изменениями, проблемами, конфигурациями, доступностью
b) реактивный
c) проактивный
d) системный
e) сервис
f) комплексный

18. Начиная с какого уровня зрелости ИТ-инфраструктуры согласно классификции компании Gartner должно обеспечиваться планирование нагрузок и емкостей, управление уровнями обслуживания
a) сервис
b) польза
c) реактивный
d) комплексный
e) оптимальный

19. Начиная с какого уровня зрелости ИТ-инфраструктуры согласно классификции компании Gartner для оценки качества ИТ-сервисов используются бизнес-метрики?
a) сервис
b) польза
c) реактивный
d) оптимальный
e) проактивный

20. Сколько профилей предприятий для оптимизации ИТ-инфраструктуры сформировала Компания IBM ?
(вводить ответ следует цифрой)

21. Компания IBM сформировала следующие профили предприятий для оптимизации ИТ-инфраструктуры:
a) товар
b) ресурс
c) клиент
d) партнер
e) поддержка

22. Для какого профиля предприятий для оптимизации ИТ-инфраструктуры (согласно классификации компании IBM) характерно, что при оптимизации ИТ-инфраструктуры в организациях с таким профилем основное внимание уделяется сокращению расходов
a) товар
b) ресурс
c) клиент
d) партнер

23. Для какого профиля предприятий для оптимизации ИТ-инфраструктуры согласно классификации компании IBM характерно, что оптимизация ИТ-инфраструктуры служит средством исполнения соглашений об уровне сервиса, сокращения времени реагирования, готовности и других параметров, связанных с обслуживанием клиентов
a) ресурс
b) товар
c) клиент
d) партнер

24. В компаниях какого профиля предприятий для оптимизации ИТ-инфраструктуры (согласно классификации компании IBM) ИТ-инициативы выступают основной движущей силой развития бизнеса и рассматриваются как необходимое условие конкурентоспособности
a) поддержка
b) партнер
c) ресурс
d) товар

25. Начиная с какого профиля предприятий для оптимизации ИТ-инфраструктуры (согласно классификации компании IBM) основное внимание уделяется получению экономического эффекта от инвестиций в информационные технологии
a) поддержка
b) партнер
c) ресурс
d) товар

26. Сколько уровней зрелости ИТ-инфраструктуры включает Модель зрелости ИТ-инфраструктуры, разработанная Microsoft ?
(вводить ответ следует цифрой)

27. Модель зрелости ИТ-инфраструктуры, разработанная Microsoft, включает следующие уровни:
a) базовый
b) динамический
c) рационализированный
d) стандартизированный
e) оптимизированный

28. На каком уровне Модели зрелости ИТ-инфраструктуры, разработанной Microsoft, начинает использоваться управление ресурсами на основе Active Directory ?

a) базовый
b) стандартизированный
c) динамический
d) рационализированный

29. На каком уровне Модели зрелости ИТ-инфраструктуры, разработанной Microsoft, предприятия с ИТ-инфраструктурой данного уровня зрелости достаточно эффективно могут управлять инцидентами, но упреждающие действия по разрешению проблем ещё не проводятся?

a) базовый
b) стандартизированный
c) динамический
d) рационализированный

30. Какой уровень Модели зрелости ИТ-инфраструктуры, разработанной Microsoft, предполагает понимание стратегической ценности ИТ для эффективного ведения бизнеса и получения конкурентных преимуществ

a) базовый
b) стандартизированный
c) динамический
d) рационализированный

31. На каком уровне Модели зрелости ИТ-инфраструктуры, разработанной Microsoft, процессы поддержки и предоставления ИТ-сервисов начинают играть важную роль в поддержке и расширении бизнеса?

a) рационализированный
b) базовый
c) стандартизированный
d) динамический

ТЕМА 5. ПРОГРАММНО-ТЕХНИЧЕСКИЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Основные вопросы темы:

1. Основные понятия и классификация средств криптографической защиты информации. Криптографические методы защиты информации. Методы стеганографии. Аппаратно-программные средства защиты информации: средства обеспечения конфиденциальности данных; средства аутентификации электронных данных и средства управления ключевой информацией. Классификация методов шифрования. Требования к современным шифрам.

2. Методы симметричного шифрования. Блочное и потоковое шифрование. Классическая сеть Фейстеля. Алгоритм шифрования DES и его модификации. Абсолютно надежный шифр. Основные свойства симметричных криптосистем.

3. Основные свойства асимметричных криптосистем. Генерация и хранение ключей. Распределение ключей. Управление ключами в системах с открытым ключом. Алгоритм Диффи-Хелмана.

4. Основные свойства хэш-функций. Основные свойства цифровой подписи. Алгоритм цифровой подписи RSA.

Рекомендации по изучению темы:

Вопрос 1 рассмотрен в учебнике [1] на с. 7-45, учебнике [5] на с. 39-39.

Вопрос 2 рассмотрен в учебнике [1] на с. 64-109, учебнике [5] на с. 39-41.

Вопрос 3 рассмотрен в учебнике [1] на с. 182-207.

Вопрос 2 рассмотрен в учебнике [1] на с. 210-226, учебнике [5] на с. 41-43.

Контрольные вопросы:

1. Как трактуются понятия «сложность вычислений» и «классы вычислений»? Дайте определения понятиям «односторонние функции», «функции с секретом», «псевдослучайные генераторы». Приведите примеры.

2. Охарактеризуйте три задачи криптографии. В чем сущность этих задач при решении проблем защиты ПО?

3. Что такое криптосинтез и криптоанализ?

4. В чем состоит основное назначение подсистем криптографической системы (подсистем шифрования, идентификации, имитозащиты, электронной подписи)?

5. Какова взаимосвязь криптографии и основных составляющих ее дисциплин?

6. Дайте определения понятиям «криптосистемы с секретным ключом», «криптосистемы с открытым ключом». Приведите примеры таких криптосистем.

7. Опишите открытое распределение ключей Диффи — Хеллмана.

8. Для чего нужны схемы электронной подписи? Приведите примеры схем электронной подписи и опишите схемы RSA, Эль-Гамаля, ГОСТ Р 34.10—2012.

9. Дайте определение понятию «криптографически стойкая хэш-функция». Опишите хэш-функции Ривеста и X.509.

10. Расскажите о сложных теоретико-числовых задачах дискретного логарифмирования и факторизации больших целых чисел. В чем их криптографический «эффект»?

11. Что называют вероятностным шифрованием? Опишите схему вероятностного шифрования.

12. Дайте определение понятию «операционная система».

13. Перечислите функции типовой операционной системы.

14. Опишите связь и интерфейсы операционной системы и прикладного ПО.

Кейсы для самостоятельной работы:

При выполнении задач предполагается, что буквы русского алфавита закодированы числа ми от до 32.

1. Определить ключ шифра Цезаря, если известны пары «открытый текст — шифро текст»:

а) апельсин — сацэнгъя;

б) засада — цоаото;

в) синица — жюгюлх;

г) ягода — дзуие;

д) лисица — гаианч.

2. Определить ключ шифрования и дешифровать сообщение, полученное шифром Цезаря:

а) арутуьчн;

б) дьюка;

в) деэаэц;

г) лдотс;

д) аратз.

3. Определить ключевое слово шифра Виженера, если известны пары «от крытый текст — шифро текст»:

а) закладка — щочэорьо;

б) лесенка — цндпцэк;

в) крокодил — ьщъкамфл;

г) серенада — йррпёлдк;

д) кукуруза — чоцвэоуо.

Тесты для самостоятельной работы:

1. Попытка шпиона передать секретную информацию на флэшке резиденту, пряча ее в специальном камне, валяющемся на обычном газоне - это
   a) физическая защита материального носителя информации от противника
   b) стеганографическая защита информации
   c) криптографическая защита информации
   d) метод социальной инженерии

2. Криптоанализ
   a) наука о снятиии криптографической защиты информации
   b) наука о криптографической защите информации
   c) наука о способах сокрытия факта передачи информации
   d) наука о способах кодирования информации

3. Согласно требований к криптографическим системам защиты информации знание противником алгоритма шифрования

a) не должно влиять на надежность защиты, обеспечиваемой любой криптографической системой
b) не должно влиять на надежность защиты, обеспечиваемой криптографической системой с симметричным шифрованием
c) не должно влиять на надежность защиты, обеспечиваемой криптографической системой с асимметричным шифрованием
d) влияет на надежность защиты, обеспечиваемой криптографической системой с асимметричным шифрованием
e) влияет на надежность защиты, обеспечиваемой криптографической системой с симметричным шифрованием

4. Аппаратным способом могут быть реализованы
a) симметричные криптоалгоритмы
b) асимметричные криптоалгоритмы

5. Программных реализации алгоритмов шифрования пл сравнению с аппаратными способами
a) являются более медленными
b) являются более быстрыми
c) обеспечивают такое же быстродействие

6. Сцитала - это
a) цилиндрический жезл определенного диаметра
b) квадрате 5x5, в который вписаны символы алфавита
c) шифровальный диск
d) тип письма, в котором буквы сближаются или соединяются одна с другой и связываются в непрерывный орнамент

7. Основоположниками асимметричного шифрования считаются
a) Диффи
b) Хеллман
c) Шиллинг
d) Шеннон
e) Эйлер

8. В соответствии с принципом Керкхоффса
a) Система шифрования должна оставаться защищённой, даже если противник полностью узнал алгоритм шифрования
b) Алгоритм шифрования должен допускать как программную, так и аппаратную реализацию
c) Система шифрования должна обеспечивать надежную защиту информации при использовании любого ключа из множества возможных
d) Система шифрования должна обеспечить приемлемое быстродействие операций шифрования и дешифрования

a) После шифрования методом Цезаря слово ШИФР превратится в: (Алфавит: АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ)
b) ЫЛЧУ
c) ЪКЦТ
d) ЬМШФ
e) ПРСТ

9. Укажите факторы успешного криптоанализа
   a) система шифрования
   b) длина перехваченного сообщения
   c) язык исходного сообщения
   d) алфавит исходного сообщения

10. При использовании шифрования с закрытым ключом какое сообщение труднее всего расшифровать
   a) с малым числом символов в сообщении и большой мощностью алфавита
   b) с малым числом символов в сообщении и малой мощностью алфавита
   c) с большим числом символов в сообщении и малой мощностью алфавита
   d) с большим числом символов в сообщении и большой мощностью алфавита

11. Перестановка бывает
   a) простая
   b) табличная
   c) многоалфавитная
   d) смысловая

12. Примеры многоалфавитной подстановки:
   a) шифр Вижинера
   b) книжный шифр
   c) шифрмашина Энигма
   d) гаммирование

13. Для какого метода замены операции шифрования и расшифрования формулируются совершенно одинаково?
   a) шифр Вижинера
   b) книжный шифр
   c) гаммирование
   d) шифр с перемешанным один раз алфавитом

14. Примеры шифров-перестановок
   a) шифр Вижинера
   b) шифр Цезаря
   c) шифр сцитала
   d) гаммирование

3. ОБЩИЕ ПОЛОЖЕНИЯ

Содержание, требования, условия и порядок организации самостоятельной работы обучающихся с учетом формы обучения определяются в соответствии с «Положением об организации самостоятельной работы обучающихся», утвержденным Ученым советом УлГУ (протокол №8/268 от 26.03.2019 г.).

Для качественного усвоения студентами материала курса при выполнении ими индивидуальных заданий необходимо, чтобы все работы выполнялись студентами после проработки соответствующего лекционного материала. Основная задача по организации учебного процесса по данной дисциплине сводится к обеспечению равномерной активной работы студентов над курсом в течение всего учебного семестра. Студенты должны регулярно прорабатывать курс прослушанных лекций, готовиться к занятиям. Для контроля качества усвоения учебного материала студентами следует проводить опросы по изученной теме. Для долговременного запоминания изученного материала следует увязывать вновь изучаемые вопросы с материалом предыдущих тем, добиваться преемственности знаний.

При выполнении заданий, вынесенных на самостоятельное изучение, необходимо наряду с библиотечным фондом пользоваться различными источниками знаний, размещенными в сети Интернет.

При изучении данного курса студентам предстоит выполнить следующие виды работ:

- Анализ теоретического материала;
- Проработка лекционного материала;
- Выполнение практических заданий (лабораторные работы);
- Подготовка к тестированию.

Лекционные занятия

Лекционные занятия желательно проводить с применением демонстрационного материала – презентации лекций на ПК с проектором. С учетом современных возможностей, желательно обеспечивать слушателей раздаточным материалом на 1-2 лекции вперед. Материал этот должен носить иллюстративный характер (схемы, графики) и ни в коем случае не подменять конспекта, который слушатель должен составлять самостоятельно.

Практические занятия

На практических занятиях решаются задачи теоретического и прикладного характера, в том числе, выполняются лабораторные работы. После каждого практического занятия следует выдавать задание на самостоятельную работу, а на следующем занятии контролировать его выполнении. Также на практических занятиях следует проводить тестирование студентов.

Текущий контроль

Для текущего контроля успеваемости (по отдельным разделам дисциплины) и промежуточной аттестации используется компьютерное тестирование, проверка реферата.

1. Планирование и организация времени, необходимого для самостоятельного изучения дисциплины.

Рекомендуется следующим образом организовать время, необходимое для изучения дисциплины:

- Изучение конспекта лекции в тот же день, после лекции: 30 минут- 1 час.
- Изучение конспекта лекции за день перед следующей лекцией: 30 минут- 1 час.
- Изучение теоретического материала по учебнику и конспекту: 1-2 часа в неделю.
- Подготовка к лабораторному занятию: 30 минут - 1 час.
- Изучение дополнительных источников, в том числе, в электронной форме: 1-2 часа в неделю.
- Всего в неделю: 1–3 часа.

2. Методические рекомендации по подготовке к практическим (лабораторным) занятиям.

По данному курсу предусмотрены лабораторные занятия. При подготовке к лабораторным занятиям следует изучить соответствующий теоретический материал по цифровой экономике, электронной коммерции, электронному бизнесу или электронным платежным системам. Теоретический материал курса становится более понятным, когда дополнительно к прослушиванию лекции и изучению конспекта, изучаются и книги по современным информационным технологиям.

Необходимо изучить лабораторную работу предыдущего занятия и выяснить те вопросы, которые показались непонятными.

Планы практических занятий, их тематика, рекомендуемая литература, цель и задачи ее изучения сообщаются преподавателем на вводных занятиях, в методических указаниях по данной дисциплине. Подготовка к практическому занятию включает 2 этапа: 1й - организационный; 2й - закрепление и углубление теоретических знаний. На первом этапе студент планирует свою самостоятельную работу, которая включает: - уяснение задания на самостоятельную работу; - подбор рекомендованной литературы; - составление плана работы, в котором определяются основные пункты предстоящей подготовки. Составление плана дисциплинирует и повышает организованность в работе. Второй этап включает непосредственную подготовку студента к занятию. Начинать надо с изучения рекомендованной литературы. Необходимо помнить, что на лекции обычно рассматривается

не весь материал, а только его часть. Остальная его часть восполняется в процессе самостоятельной работы. В связи с этим работа с рекомендованной литературой обязательна. Особое внимание при этом необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения рассматриваемых теоретических вопросов. В процессе этой работы студент должен стремиться понять и запомнить основные положения рассматриваемого материала, примеры, поясняющие его, а также разобраться в иллюстративном материале. Заканчивать подготовку следует составлением плана (конспекта) по изучаемому материалу (вопросу). Это позволяет составить концентрированное, сжатое представление по изучаемым вопросам. В процессе подготовки к занятиям рекомендуется взаимное обсуждение материала, во время которого закрепляются знания, а также приобретается практика в изложении и разъяснении полученных знаний, развивается речь. При необходимости следует обращаться за консультацией к преподавателю. Идя на консультацию, необходимо хорошо продумать вопросы, которые требуют разъяснения. В начале занятия студенты под руководством преподавателя более глубоко осмысливают теоретические положения по теме занятия, раскрывают и объясняют основные положения публичного выступления. В процессе творческого обсуждения и дискуссии вырабатываются умения и навыки использовать приобретенные знания для различного рода ораторской деятельности. Записи имеют первостепенное значение для самостоятельной работы студентов. Они помогают понять построение изучаемого материала, выделить основные положения, проследить их логику и тем самым проникнуть в творческую лабораторию автора. Ведение записей способствует превращению чтения в активный процесс, мобилизует, наряду со зрительной, и моторную память. Следует помнить: у студента, систематически ведущего записи, создается свой индивидуальный фонд подсобных материалов для быстрого повторения прочитанного, для мобилизации накопленных знаний. Особенно важны и полезны записи тогда, когда в них находят отражение мысли, возникшие при самостоятельной работе. Важно развивать у студентов умение сопоставлять источники, продумывать изучаемый материал. Большое значение имеет совершенствование навыков конспектирования у студентов. Преподаватель может рекомендовать студентам следующие основные формы записи: план (простой и развернутый), выписки, тезисы. Результаты конспектирования могут быть представлены в различных формах. План - это схема прочитанного материала, краткий (или подробный) перечень вопросов, отражающих структуру и последовательность материала. Подробно составленный план вполне заменяет конспект. Конспект - это систематизированное, логичное изложение материала источника. Различаются четыре типа конспектов:

- План-конспект - это развернутый детализированный план, в котором достаточно подробные записи приводятся по тем пунктам плана, которые нуждаются в пояснении.
- Текстуальный конспект - это воспроизведение наиболее важных положений и фактов источника.
- Свободный конспект - это четко и кратко сформулированные (изложенные) основные положения в результате глубокого осмысливания материала. В нем могут присутствовать выписки, цитаты, тезисы; часть материала может быть представлена планом.
- Тематический конспект - составляется на основе изучения ряда источников и дает более или менее исчерпывающий ответ по какой-то схеме (вопросу).

3. Групповая консультация

Разъяснение является основным содержанием данной формы занятий, наиболее сложных вопросов изучаемого программного материала. Цель - максимальное приближение обучения к практическим интересам с учетом имеющейся информации и является результативным материалом закрепления знаний. Групповая консультация проводится в следующих случаях:

- когда необходимо подробно рассмотреть практические вопросы, которые были недостаточно освещены или совсем не освещены в процессе лекции;
- с целью оказания помощи в самостоятельной работе (написание рефератов, выполнение курсовых работ, сдача экзаменов, подготовка конференций);
- если студенты самостоятельно изучают нормативный, справочный материал, инструкции, положения.