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 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Ульяновск, 2019

Методические указания для самостоятельной работы студентов по дисциплине «Информационная безопасность» / составитель: А.Г. Сковиков. - Ульяновск: УлГУ, 2019.

Настоящие методические указания предназначены для студентов бакалавриата по направлению 38.03.05 «Бизнес-информатика» (степень – бакалавр), изучающих дисциплину «Информационная безопасность». 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. Студентам очной формы обучения они будут полезны 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

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ

ТЕМА 1. ВВЕДЕНИЕ В ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ.

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. МОДЕЛИ ХРАНЕНИЯ ДАННЫХ.

Основные вопросы темы:

1. Этапы жизненного цикла информационных систем и меры безопасности. Что такое законодательный уровень информационной безопасности и почему он важен. Обзор российского законодательства в области информационной безопасности. Правовые акты общего назначения, затрагивающие вопросы информационной безопасности.

2. Обзор зарубежного законодательства в области информационной безопасности. О текущем состоянии российского законодательства в области информационной безопасности. Понятие стандарта. Классификация стандартов в области информационной безопасности. «Оранжевая книга», ее структура и группы классов защищенности.

Рекомендации по изучению темы:

Вопрос 1 рассмотрен в учебнике [5] на с. 181-189, учебнике [7] на с. 40-114.

Вопрос 2 рассмотрен в учебнике [6] на с. 32-35, учебнике [7] на с. 130-156.

Контрольные вопросы:

1. На достижение каких целей ориентирована государственная политика в области обеспечения национальной безопасности?
2. Что является стратегическими национальными приоритетами России в области национальной безопасности?
3. Каковы приоритеты устойчивого развития общества?
4. Какие факторы обусловливают влияние информационной безопасности на национальную безопасность?
5. Раскройте основные содержание понятия «информационная инфраструктура».
6. Что такое «угрозы безопасности информационной инфраструктуры» и какие угрозы вы знаете?
7. Какова общая структура правовых средств противодействия угрозам безопасности информационной инфраструктуры?
8. Расскажите об основных формах существования и свойствах информации.
9. Раскройте особенности основных видов информации как объектов обеспечения безопасности.
10. Каковы основные угрозы безопасности информации и способы их возможного проявления?
11. Расскажите об основных источниках права в области обеспечения безопасности информации.
12. Раскройте понятие «правового режима безопасности информации» и его содержание.
13. Раскройте содержание организационного обеспечения информационной безопасности Российской Федерации.
14. Какова система организационного обеспечения информационной безопасности?
15. Перечислите основные документы стратегического планирования.
16. Расскажите об основных уполномоченных федеральных органах исполнительной власти в области информационной безопасности."
17. Что является стратегическими национальными приоритетами России в области национальной безопасности?
18. Каковы приоритеты устойчивого развития общества?
19. Какие факторы обусловливают влияние информационной безопасности на национальную безопасность?
20. Раскройте основные содержание понятия «информационная инфраструктура».

21. Что такое «угрозы безопасности информационной инфраструктуры» и какие угрозы вы знаете?

22. Какова общая структура правовых средств противодействия угрозам безопасности информационной инфраструктуры?

23. Расскажите об основных формах существования и свойствах информации.

24. Раскройте особенности основных видов информации как объектов обеспечения безопасности.

25. Каковы основные угрозы безопасности информации и способы их возможного проявления?

26. Расскажите об основных источниках права в области обеспечения безопасности информации.

27. Раскройте понятие «правового режима безопасности информации» и его содержание.

28. Раскройте содержание организационного обеспечения информационной безопасности Российской Федерации.

29. Какова система организационного обеспечения информационной безопасности?

30. Перечислите основные документы стратегического планирования.

31. Расскажите об основных уполномоченных федеральных органах исполнительной власти в области информационной безопасности.

32. Назовите основополагающие международные правовые акты в области международной информационной безопасности.

33. Какие вы знаете региональные международные организации и соглашения (договоры) в области МИБ?

34. Какие тенденции и проблемы МИБ имеются сегодня?

35. Охарактеризуйте положительный зарубежный опыт в этой сфере.

36. Какие инициативы выдвинуты Россией в области МИБ?

37. Охарактеризуйте основные положения Указа Президента РФ от 22.05.2015 № 260.

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. 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

2. 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

3. 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.

4. 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. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА АДМИНИСТРАТИВНОМ УРОВНЕ.

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. Разработать ER-модель предметной области, описанной в проектах 1 или 2 в теме №1. Каждую сущность охарактеризовать набором атрибутов.

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 x Риски x Ценность актива
   b) (Угрозы x Ценность актива x Уязвимости) x Риски
   c) SLE x Частоту = ALE
   d) (Угрозы x Уязвимости x Ценность актива) x 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

ТЕМА 4. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРОЦЕДУРНОМ УРОВНЕ.

Основные вопросы темы:

1. Основные классы мер процедурного уровня: управление персоналом; физическая защита; поддержание работоспособности; реагирование на нарушения режима безопасности; планирование восстановительных работ.

Рекомендации по изучению темы:

Вопрос 1 рассмотрен в учебном пособии [2] на с. 14-21, 126-139; 130-144.

Контрольные вопросы:

1. Перечень основных организационных работ по защите информации.
2. Структура и функции органов защиты информации.
3. Список документационного обеспечения работ по защите информации.
4. Перечислите меры физической защиты данных.
5. В чем суть сервиса информационной безопасности - поддержание работоспособности?

Кейсы для самостоятельной работы:

1. Преобразовать ER-модель в реляционную модель. Полученные таблицы проверить на соответствие требованиям 1НФ, 2НФ, 3НФ.

Тесты для самостоятельной работы:

1. Укажите элементы реляционной модели
   a) Отношение
   b) Схема отношения
   c) Тип данных
   d) Состояние объекта
   e) Набор

2. Что такое процедура?
   a) Правила использования программного и аппаратного обеспечения в компании
   b) Пошаговая инструкция по выполнению задачи
   c) Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах
   d) Обязательные действия

3. Что такое политики безопасности?
   a) Пошаговые инструкции по выполнению задач безопасности
   b) Общие руководящие требования по достижению определенного уровня безопасности
   c) Широкие, высокоуровневые заявления руководства
   d) Детализированные документы по обработке инцидентов безопасности

4. Эффективная программа безопасности требует сбалансированного применения:
   a) Технических и нетехнических методов
   b) Контрмер и защитных механизмов
   c) Физической безопасности и технических средств защиты
   d) Процедур безопасности и шифрования

5. 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

6. Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:
   a) черный пиар
   b) фишинг
   c) нигерийские письма
   d) источник слухов
   e) пустые письма

7. Что понимается под совокупностью документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов?
   a) информационная политика
   b) безопасность информации
   c) политика безопасности
   d) регламентация доступа
   e) организация защиты

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 Х.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.