Министерство науки и высшего образования РФ
ФГБОУ ВО «Ульяновский государственный университет»
Факультет математики, информационных и авиационных технологий

Иванцов А.М.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ПО ДИСЦИПЛИНЕ «ВВЕДЕНИЕ В СПЕЦИАЛЬНОСТИ НАУЧНО-ОБРАЗОВАТЕЛЬНОГО КЛАСТЕРА»

Для студентов специалитета по специальностям 10.05.01 и 10.05.03
очной формы обучения

Ульяновск, 2022

Методические указания для самостоятельной работы студентов по дисциплине «Введение в специальности научно-образовательного кластера» / составитель: А.М. Иванцов. - Ульяновск: УлГУ, 2022. Настоящие методические указания предназначены для студентов специалитета по специальностям 10.05.01 и 10.05.03 очной формы обучения. В работе приведены литература по дисциплине, основные темы курса и вопросы в рамках каждой темы, рекомендации по изучению теоретического материала, контрольные вопросы для самоконтроля и тесты для самостоятельной работы. Студентам очной формы обучения они будут полезны при подготовке к зачёту по данной дисциплине.

Рекомендованы к введению в образовательный процесс Ученым советом факультета математики, информационных и авиационных технологий УлГУ (протокол № 3/22 от 19.04.2022 г.).

Содержание

1. ЛИТЕРАТУРА ДЛЯ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

1. Малюк А.А., Введение в информационную безопасность [Электронный ресурс]: Учебное пособие для вузов / А.А. Малюк, В.С. Горбатов, В.И. Королев и др.. Под ред. В.С. Горбатова. - М.: Горячая линия - Телеком, 2011. - 288 с. - ISBN 978-5-9912-0160-5 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991201605.html.

2. Трушин В.А., Введение в информационную безопасность и защиту информации [Электронный ресурс]: учебное пособие / Трушин В.А. - Новосибирск: Изд-во НГТУ, 2017. - 132 с. - ISBN 978-5-7782-3233-4 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785778232334.html.

3. Некоммерческая интернет-версия СПС "КонсультантПлюс":

3.1 Доктрина информационной безопасности Российской Федерации (Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации")
Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_208191/

3.2 Стратегия национальной безопасности Российской Федерации (Указ Президента Российской Федерации от 02.07.2021 года N 400 "О Стратегии национальной безопасности Российской Федерации") Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_191669/

3.3 Закон Российской Федерации от 21.07.1993 № 5485-I «О государственной тайне». Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_2481/

3.4. Федеральный закон от 27.06.2006 N149-ФЗ "Об информации, информационных технологиях и защите информации"
Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/

3.5 Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/

3.6 Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»
Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48699/

3.7 Федеральный государственный образовательный стандарт высшего образования по специальности 10.05.01 «Компьютерная безопасность (уровень специалитета). Приказ Министерства науки и высшего образования от 26.10.2020 г. N 1459.

3.8 Федеральный государственный образовательный стандарт высшего образования по специальности 10.05.03 Информационная безопасность автоматизированных систем (уровень специалитета). Приказ Министерства науки и высшего образования от 26.10.2020 г. N 1457.

4. Дронов В.Ю., Международные и отечественные стандарты по информационной безопасности [Электронный ресурс]: Дронов В.Ю. - Новосибирск: Изд-во НГТУ, 2016. - 34 с. - ISBN 978-5-7782-3112-2 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785778231122.html.

5. Методические указания по написанию курсовых и дипломных работ для студентов специальности «Компьютерная безопасность» / А.С. Андреев,

А.М. Иванцов, С.М. Рацеев.– Ульяновск: УлГУ, 2017. – 40 с. URL:ftp://10.2.5.225/FullText/Text/Andreev_2017.pdf.

6. Основы информационной безопасности. Курс лекций. Часть 1 / А.М. Иванцов, В.Г. Козловский. – Ульяновск: УлГУ, 2020 – 63 с.

7. Основы информационной безопасности. Курс лекций. Часть 2 / А.М. Иванцов, В.Г. Козловский. – Ульяновск: УлГУ, 2020 – 103 с.

8. Профессиональная этика и психология делового общения: учебное пособие / И.П.Кошевая, А.А. Канке. - М.: ИД "Форум": ИНФРА-М, 2013. - 304с.

9. Информационная безопасность компьютерных систем и сетей: учебное пособие / В.Ф. Шаньгин. – М.: ИД «ФОРУМ»; ИНФРА-М, 2014. – 416 с. ил.

10. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации: Учебное пособие. - 2-е изд. - М.: РИОР: ИНФРА-М, 2015. - 392с.

11. Новиков В.К., Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации) [Электронный ресурс]: Учебное пособие. / В.К. Новиков - М.: Горячая линия - Телеком, 2015. - 176 с. - ISBN 978-5-9912-0525-2 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991205252.html.

12. Инженерно-техническая защита информации: учебное пособие для студентов, обучающихся по специальностям в области информационной безопасности / А.А. Торокин. М.: Гелиос АРВ, 2005, 960 с.

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ

2.1. РАЗДЕЛ 1. ОБЩАЯ ХАРАКТЕРИСТИКА СПЕЦИАЛЬНОСТЕЙ 10.00.00

ТЕМА 1. ВВЕДЕНИЕ В ДИСЦИПЛИНУ. ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ ИБ

Основные вопросы:

1. Сущность и содержание национальной безопасности
2. Основные понятия и общеметодологические принципы ИБ
3. Базовые понятия и определения информационной безопасности
4. Основные принципы организации защиты информации

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [6] на с. 6-10.

Для самостоятельного изучения вопроса 1 следует обратиться к [3.1-3.6]

Вопрос 2 изложен в учебном пособии [1] на с. 11-14.

Для самостоятельного изучения вопроса 2 следует обратиться к [3.1- 3.6].

Вопрос 3 изложен в лекции, в [3.1, 3.2, 1, 2, 8].

Для самостоятельного изучения вопроса 3 следует обратиться к [3.1- 3.3].

Вопрос 4 изложен в лекции.

Контрольные вопросы по теме 1:

1. В чём заключаются особенности существующей в России системы обеспечения национальной безопасности?
2. Перечислить основные задачи по обеспечению национальной безопасности Российской Федерации.
3. Пояснить понятия субъекта и объекта безопасности.
4. Основные элементы национальной безопасности.
5. Виды безопасности. Классификация видов национальной безопасности по характеру угроз.
6. Классификация видов национальной безопасности по сферам жизнедеятельности.
7. Основные принципы Государственной политики обеспечения информационной безопасности (ИБ) РФ.
8. Основные составляющие ИБ.
9. Перечень оснований для ограничения информационных прав.
10. Перечень случаев прямого ограничения информационных прав.
11. Перечень видов информации с ограниченным доступом.
12. Предметы рассмотрения дисциплины.
13. Основные базовые свойства защищаемой информации.
14. Основные цели защиты информации (ЗИ).
15. Основная терминология по ИБ и ЗИ.
16. Основные принципы организации ЗИ.

Тесты для самостоятельной работы:

1. **Какой из документов, где изложены направления и задачи по обеспечению национальной безопасности, является действующим?**

а) Стратегии нац. безопасности РФ
б) Концепция национальной безопасности РФ
в) Стратегия национальной безопасности РФ до 2020 года

2. **Что не относится к основным задачам в области обеспечения национальной безопасности РФ?**

а) Реализация оперативных и долгосрочных мер по предупреждению и нейтрализации внутренних и внешних угроз
б) Обеспечение на территории России личной безопасности человека и гражданина, его конституционных прав и свобод
в) Формирование культуры людей в области информационной безопасности
г) Подъем экономики страны, проведение независимого и социально ориентированного экономического курса

3. **Какой документ определяет действующий официальный термин «национальная безопасность»?**

а) Стратегии нац. безопасности РФ
б) Доктрина информационной безопасности РФ
в) Конституции РФ

4. **Какой документ определяет действующий официальный термин «Информационная безопасность»?**

а) Стратегии нац. безопасности РФ
б) Доктрина информационной безопасности РФ
в) Закон РФ «О безопасности».
г) Конституции РФ

5. **Какое из базовых свойств защищаемой информации является основным для специалистов отдела информационных технологий?**

а) Конфиденциальность
б) Доступность
в) Целостность

2.2. РАЗДЕЛ 1. ОБЩАЯ ХАРАКТЕРИСТИКА СПЕЦИАЛЬНОСТЕЙ 10.00.00

ТЕМА 2. НАЗНАЧЕНИЕ И СТРУКТУРА ФЕДЕРАЛЬНЫХ ГОСУДАРСТВЕННЫХ ОБРАЗОВАТЕЛЬНЫХ СТАНДАРТОВ ВЫСШЕГО ОБРАЗОВАНИЯ (ФГОС ВО) 10.05.03 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ» И 10.05.01 «КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ». КВАЛИФИКАЦИОННАЯ ХАРАКТЕРИСТИКА СПЕЦИАЛИСТА ПО ЗАЩИТЕ ИНФОРМАЦИИ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО ОБРАЗОВАТЕЛЬНОГО СТАНДАРТА ВЫСШЕГО ОБРАЗОВАНИЯ (ФГОС ВО)

Основные вопросы:

1. Характеристика специальностей 10.05.01 (10.05.03)
2. Требования к структуре и условиям реализации программы специалитета 10.05.01 (10.05.03)

Рекомендации по изучению темы:

Вопрос 1 изложен в лекции.

Для самостоятельного изучения вопроса 1 следует обратиться к [3.7-3.8].

Вопрос 2 изложен в лекции.

Для самостоятельного изучения вопроса 2 следует обратиться к [3.7-3.8].

Контрольные вопросы по теме 2

1. Объём и продолжительность программы специалитета 10.05.01 (10.05.03).
2. Область профессиональной деятельности выпускников, освоивших программу специалитета 10.05.01 (10.05.03).
3. Объекты профессиональной деятельности выпускников, освоивших программу специалитета 10.05.01 (10.05.03).
4. Специализации, по которым готовятся выпускники, освоившие программу специалитета 10.05.01 (10.05.03).
5. Какие профессиональные задачи должен решать выпускник, освоивший программу специалитета 10.05.01 (10.05.03).
6. Требования к структуре и условиям реализации программы специалитета 10.05.01 (10.05.03).

Тесты для самостоятельной работы:

1. Какая специализация специальности "Информационная безопасность автоматизированных систем" осваивается в УлГУ?

а) Информационная безопасность автоматизированных. систем критически важных объектов.

б) Безопасность открытых информационных систем"

в) Информационная безопасность автоматизированных банковских систем.

г) Защищенные автоматизированные системы управления.

2. Какая специализация специальности «Компьютерная безопасность» осваивается в УлГУ?

а) Анализ безопасности компьютерных систем

б) Математические методы защиты информации

в) ИБ объектов информатизации на базе компьютерных систем

г) Безопасность распределенных компьютерных систем

2.3 РАЗДЕЛ 1. ОБЩАЯ ХАРАКТЕРИСТИКА СПЕЦИАЛЬНОСТЕЙ 10.00.00

ТЕМА 3. УЧЕБНЫЙ ПЛАН ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО СПЕЦИАЛЬНОСТЯМ 10.05.03. И 10.05.01. СОСТАВ И НАЗНАЧЕНИЕ ОСНОВНЫХ ДИСЦИПЛИН ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ. СОСТАВ И НАЗНАЧЕНИЕ ОСНОВНЫХ ДИСЦИПЛИН ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Основные вопросы:

1. Характеристика учебного плана подготовки специалистов по специальности 10.05.01 (10.05.03)
2. Характеристика и место дисциплин в подготовке специалитета 10.05.01 (10.05.03)

Рекомендации по изучению темы:

Вопрос 1 изложен в лекции.

Для самостоятельного изучения вопроса 1 следует обратиться к учебному плану подготовки специалистов по специальности 10.05.01 (10.05.03) на сайте УлГУ и к [3.7-3.8].

Вопрос 2 изложен в лекции.

Для самостоятельного изучения вопроса 1 следует обратиться к учебному плану подготовки специалистов по специальности 10.05.01 (10.05.03) на сайте УлГУ и к [3.7-3.8].

Контрольные вопросы по теме 3:

1. Какие блоки (модули дисциплин) включены в учебный план по программе специалитета 10.05.01 (10.05.03)?
2. Перечислить дисциплины по выбору для программы специалитета 10.05.01 (10.05.03).
3. В каких семестрах для программы специалитета 10.05.01 (10.05.03) запланированы практики?
4. Какой объём времени в учебном плане по программе специалитета 10.05.01 (10.05.03) отведён для государственной итоговой аттестации?
5. Назвать дисциплины факультативов для учебного плана по программе специалитета 10.05.01 (10.05.03).
6. По каким дисциплинам и в какие семестры запланированы курсовые работы для учебного плана по программе специалитета 10.05.01 (10.05.03).

7. Какие кафедры осуществляют подготовку студентов специалитета 10.05.01 (10.05.03) по специальным дисциплинам?

Тесты для самостоятельной работы:

1. Каков максимальный и минимальный объёмы контактной работы со студентами в неделю? 16,36

а) 16, 36
б) 12, 48
в) 16, 52

2. Какова максимальная учебная нагрузка в неделю?

а) 75
б) 62
в) 42

2.4. РАЗДЕЛ 1. ОБЩАЯ ХАРАКТЕРИСТИКА СПЕЦИАЛЬНОСТЕЙ 10.00.00

ТЕМА 4. ТРЕБОВАНИЯ К УРОВНЮ ПОДГОТОВКИ СПЕЦИАЛИСТА. ОРГАНИЗАЦИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА В УНИВЕРСИТЕТЕ

Основные вопросы:

1. Знания и умения выпускников специалитета 10.05.01 (10.05.03)
2. Требования к курсовым работам, рефератам, к государственной итоговой аттестации выпускников специалитета 10.05.01 (10.05.03)
3. Виды учебных занятий. Сущность и назначение лекционных, семинарских, практических, лабораторных занятий, учебных, производственных и преддипломных практик
4. Система организации студенческой научно-исследовательской работы

Рекомендации по изучению темы:

Вопрос 1 изложен в лекции.

Для самостоятельного изучения вопроса 1 следует обратиться к [3.7-3.8].

Вопрос 2 изложен в лекции.

Для самостоятельного изучения вопроса 2 следует обратиться к учебному пособию [5].

Вопрос 3 изложен в лекции.

Для самостоятельного изучения вопроса 1 следует обратиться к [3.7-3.8].

Вопрос 4 изложен в лекции.

Для самостоятельного изучения вопроса 1 следует обратиться к [3.7-3.8].

Контрольные вопросы по теме 5:

1. Какие виды компетенций используются в стандарте специалитета 10.05.01 (10.05.03)?
2. Какие виды компетенций предлагается использовать в стандарте в 3++ специалитета 10.05.01 (10.05.03)?
3. Какие основные общекультурные компетенции должен освоить выпускник специалитета?
4. Какие основные общепрофессиональные компетенции должен освоить выпускник специалитета?
5. Какие основные общепрофессиональные компетенции должен освоить выпускник специалитета?
6. Какие основные профессиональные компетенции должен освоить выпускник специалитета?
7. Какие основные профессионально-специализированные компетенции должен освоить выпускник специалитета?
8. Перечислить основные требования к курсовым работам и рефератам.
9. Сущность и назначение лекционных, семинарских, практических, лабораторных занятий.
10. Сущность и назначение учебных, производственных и преддипломных практик.

Перечислить основные требования к организации студенческой научно-исследовательской работы в УлГУ.

Тесты для самостоятельной работы:

1. Какой вид компетенций, из названных, отсутствует в стандарте ФГОС 3+ относительно проекта стандарта 3++?

а) ОПК
б) ПК
в) УК
г) ПСК

2.5. РАЗДЕЛ 2. ОСНОВНЫЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ТЕМА 5. ОСНОВЫ ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ. ОСНОВНЫЕ НОРМАТИВНЫЕ ДОКУМЕНТЫ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Основные вопросы:

1. Информация как объект правоотношений
2. Виды и содержание тайн

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [9] на с. 9-15, в учебном пособии [10] на с. 8-13.

Для самостоятельного изучения вопроса 1 следует обратиться к [11] на с. 3-10 и к [3.1-3.6, 11].

Вопрос 2 изложен в лекции.

Для самостоятельного изучения вопроса 2 следует обратиться к [10] на с. 62-71.

Контрольные вопросы по теме 5:

1. Основные объекты обеспечения информационной безопасности (ИБ).
2. Основные субъекты обеспечения ИБ.
3. Перечислить основные предметные области информационной сферы.
4. Законодательная основа информационной безопасности (Конституция Российской Федерации, Законы и Кодексы РФ).
5. Основные положения Федерального Закона «Об информации, информационных технологиях и о защите информации».
6. Основные положения закона РФ «О государственной тайне»
7. Основные положения Федерального Закона "О персональных данных".
8. Основные положения Федерального Закона "О коммерческой тайне".
9. Основные организационные и правовые меры режима коммерческой тайны.

Тесты для самостоятельной работы:

1. В каком нормативно-правовом акте дана трактовка понятия «информация»?

а) в Федеральном Законе «О персональных данных»

б) в Федеральном Законе «Об информации, информационных технологиях и о защите информации»

в) в Федеральном Законе «О коммерческой тайне»

г) в Доктрине информационной безопасности РФ

2. Какой документ определяет национальные интересы РФ в информационной сфере?
а) Доктрина информационной безопасности
б) Конституция РФ
в) № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
г) Закон РФ N 5485-1 «О государственной тайне»

3. К какой области относятся сведения о силах и средствах гражданской обороны?
а) Сведения в военной области
б) Сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности
в) Сведения в области экономики, науки и техники

4. Кто является обладателем информации, составляющей коммерческую тайну, полученной в рамках трудовых отношений?
а) Работник
б) Работодатель
в) Пенсионный фонд
г) Налоговая служба

2.6. РАЗДЕЛ 2. ОСНОВНЫЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ТЕМА 6. ОСНОВНЫЕ МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Основные вопросы:

1. Идентификация и аутентификация
2. Разграничение доступа
3. Регистрация и аудит
4. Криптография
5. Экранирование

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [7] на с. 57-60.
Для самостоятельного изучения вопроса 1 следует обратиться к [11, 12]
Вопрос 2 изложен в учебном пособии [7] на с. 57-60, 69-70.
Вопрос 3 изложен в лекции.
Вопрос 4 изложен в учебном пособии [7] на с. 30-38.
Вопрос 5 изложен в учебном пособии [7] на с. 70-87.

Контрольные вопросы по теме 6:

1. Дать определение идентификации и аутентификации субъектов и объектов информационных систем.
2. Что такое авторизация?
3. Привести вариант классификации систем и методов аутентификации.
4. Методы аутентификации, основанные на паролях.
5. Методы аутентификации, основанные на измерении биометрических параметров человека.
6. Строгие методы аутентификации.
7. Основные методы разграничения доступа.
8. Сущность дискреционного управления доступом.
9. Сущность мандатного управления доступом.
10. Основные цели реализации механизмов регистрации и аудита.
11. Практические средства регистрации и аудита.
12. Основных методы шифрования
13. Контроль целостности информации.
14. Основные методы контроля целостности
15. Межсетевые экраны. Основные понятия.

Тесты для самостоятельной работы:

1. Какое из утверждений относится к мандатным моделям управления доступом?

а) Модель, в которой владелец ресурса сам задает права доступа к нему
б) Модель, копирующая иерархическую структуру организации и позволяющая упростить администрирование
в) Модель, в которой режим доступа субъектов к объектам определяется установленным режимом конфиденциальности
г) Модель являющаяся наиболее универсальной и позволяющая контролировать доступ с учетом произвольных параметров среды, субъектов и объектов доступа

2. Какое из утверждений относится к дискреционным моделям управления доступом?

а) Модель, в которой владелец ресурса сам задает права доступа к нему
б) Модель, копирующая иерархическую структуру организации и позволяющая упростить администрирование
в) Модель, в которой режим доступа субъектов к объектам определяется установленным режимом конфиденциальности
г) Модель, являющаяся наиболее универсальной и позволяющая контролировать доступ с учетом произвольных параметров среды, субъектов и объектов доступа

3. Что, из перечисленного, не является сферой применения криптографии?

а) Обслуживание банковских пластиковых карт
б) Хранение и обработка паролей пользователей в сети
в) Сдача бухгалтерских и иных отчетов через удаленные каналы связи

г) Использование цифровых водяных знаков

4. Что такое идентификация?
а) Процедура проверки подлинности заявленного пользователя, процесса или устройства
б) Процедура распознавания пользователя по его имени
в) Процедура предоставления субъекту определенных полномочий и ресурсов в данной системе

5. Задачей средств ограничения доступа является:
а) Исключить случайный и преднамеренный доступ посторонних лиц на территорию размещения КСА и непосредственно к аппаратуре
б) Создать некоторые преграды вокруг объекта защиты
в) Использовать цепи сигнализации и индикации в комплексе с различными датчиками

2.7. РАЗДЕЛ 2. ОСНОВНЫЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ТЕМА 7. ОСНОВНЫЕ ПОНЯТИЯ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Основные вопросы:

1. Основные понятия криптографии. История криптографии
2. Обобщенные схемы симметричной и ассимметричной криптосистем

Рекомендации по изучению темы:
Вопрос 1 изложен в учебном пособии [7] на с. 30-35.
Вопрос 2 изложен в учебном пособии [7] на с. 38-43, 47-52.

Контрольные вопросы по теме 7:

1. История криптографии. Основные методы защиты секретов.
2. Основные понятия криптографии.
3. Основные задачи криптографии.
4. Разделы криптографии.
5. Что такое электронная подпись (ЭП)?
6. Принцип работы роторных шифровальных машин.
7. Обобщенная схема симметричной криптосистемы.
8. Обобщенная схема ассимметричной криптосистемы.

Тесты для самостоятельной работы:

1. Дешифрование это:
а) процесс расшифрования без знания ключа
б) процесс, обратный шифрованию

2. Какая проблема является наиболее актуальной для симметричных криптосистем?

а) проблема безопасного распределения симметричных секретных ключей

б) проблема использования ресурсоемких операций

в) проблема реализации аппаратного шифратора

3. Какое требование, из перечисленных, не характерно для асимметричной криптосистемы?

а) вычисление пары ключей (Kb и кb) получателем B (на основе начального условия) должно быть достаточно сложным

б) отправитель A, зная открытый ключ Kb и сообщение M, может легко вычислить криптограмму C=EKb(M)

в) получатель B, используя секретный ключ кb и криптограмму C, может легко восстановить исходное сообщение M=Dкb(C)

г) противник, зная открытый ключ Kb, при попытке вычислить секретный, ключ кb, (наталкивается на непреодолимую вычислительную проблему

2.8. РАЗДЕЛ 2. ОСНОВНЫЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ТЕМА 8. ИДЕНТИФИКАЦИЯ, АУТЕНТИФИКАЦИЯ И КОНТРОЛЬ ДОСТУПА К ИНФОРМАЦИИ

Основные вопросы:

1. Основы идентификации и аутентификации
2. Классификация протоколов аутентификации

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [7] на с. 57-60.

Вопрос 2 изложен в учебном пособии [7] на с. 60-64.

Контрольные вопросы по теме 8:

1. Понятия идентификации, аутентификации, авторизации и администрирования.
2. Пояснить процесс идентификации и аутентификации.
3. Рассмотреть категории процессов аутентификации.
4. Основные характеристики протоколов аутентификации.
5. Методы аутентификации, использующие пароли и PIN-коды.
6. Строгая аутентификация на основе использования криптографических методов и средств.
7. Биометрическая аутентификация.

Тесты для самостоятельной работы:

1. Что из перечисленного относится к администрированию?

а) Регистрация действий пользователя в сети, включая его попытки доступа к

ресурсам
б) Процедура проверки подлинности заявленного пользователя, процесса или устройства
в) Процедура распознавания пользователя по его имени

2. Что, из перечисленного, обычно не используется в качестве биометрических признаков при аутентификации потенциального пользователя
а) Отпечатки пальцев
б) Форма и размеры лица
в) Отпечаток стопы
г) Особенности голоса