ГОУ ВПО Российско-Армянский (Славянский) университет

Утверждено
Директор Института
_____ Агаронян А.К.

«11» июня 2024 г., протокол № 38
Утвержден Ученым Советом ИФИ

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДИСЦИПЛИНЫ

Наименование дисциплины: Б1.В.ДВ.03.01«Информационные технологии в коммуникации»

Автор (ы) ***доцент, кандидат тех. наук, Бадалян Б.Ф***
Ф.И.О, ученое звание (при наличии), ученая степень (при наличии)

Направление подготовки: 11.03.02 Инфокоммуникационные технологии и системы связи

1. АННОТАЦИЯ

1.1. Краткое описание содержания данной дисциплины;

В курсе дисциплины “Информационные технологии в коммуникации” изучаются основные проблемы мониторинга и аудита безопасности в инфокоммуникационных системах. Рассматриваются методы аутентификации пользователей как на основе парольных, так и биометрических систем, а также излагаются основные понятия информационной безопасности, необходимые для профессиональной деятельности в области информационных и коммуникационных технологий. Приводятся основные методы ,средства и механизмы выявления уязвимостей в защите телекоммуникационных систем и сетей. Даны определения и примеры криптографического закрытия информации. Подробно рассмотрены классические и современные симметричные и асимметричные криптосистемы шифрования, методы создания цифровой подписи, схемы практической реализации популярных помехоустойчивых кодов, специальные технические средства для выявления источников киберслежки. Описываются процедуры аутентификации, шифрования и помехоустойчивого кодирования в современных телекоммуникационных системах и стандартах.

1.2. Трудоемкость в академических кредитах-3, в часах-108, форма итогового контроля-зачет;

1.3. Данная дисциплина теснейшим образом связана со следующими дисциплинами: теория вероятностей и математическая статистика, общая теория связи, основы теории связи с подвижными объектами, цифровая обработка сигналов.

1.4. Результаты освоения программы дисциплины:

Код компетенции *(в соответствии рабочим с учебным планом)*	**Наименование компетенции** *(в соответствии рабочим с учебным планом)*	**Код индикатора достижения компетенций** *(в соответствии рабочим с учебным планом)*	**Наименование индикатора достижений компетенций***(в соответствии рабочим с учебным планом)*
УК-1	***Способен осуществлять поиск, критический анализ и синтез информации, применять системный***	УК-1.1	**Знает** методики поиска, сбора и обработки информации, метод

	подход для решения поставленных задач.		системного анализа
		УК-1.2	**Умеет** применять методики поиска, сбора и обработки информации, осуществлять критический анализ и синтез информации, полученной из разных источников, применять системный подход для решения поставленных задач.
		УК-1.3	**Владеет** методами поиска, сбора и обработки, критического анализа и синтеза информации, методикой системного подхода для решения поставленных задач.
ПК-3	***Способен применять современные теоретические и экспериментальные методы исследования с целью создания новых перспективных средств инфокоммуникаций, использованию и внедрению результатов исследований.***	**ПК-3.1**	**Знает** основы сетевых технологий, нормативно-техническую документацию, требования технических регламентов, международные и национальные стандарты в области качественных показателей работы инфокоммуникационного оборудования.
		ПК-3.2	**Умеет** работать с программным обеспечением, используемым при обработке информации инфокоммуникационных систем и их составляющих.
		ПК-3.3	**Владеет** навыками анализа оперативной информации о запланированных и аварийных работах, связанных с прерыванием предоставления услуг,

			контроля качества предоставляемых услуг.
ПК-4	***Способен к составлению аналитических отчетов на основе аналитического и численного исследования рынка и построению прогнозов по продажам инфокоммуникационных систем и/или их составляющих.***	**ПК-4.1**	**Знает** основы инфокоммуникационных технологий и способы поиска информации по продажам инфокоммуникационных систем и/или их составляющих.
		ПК-4.2	**Умеет** применять системы управления взаимоотношениями с клиентами при подготовке аналитических отчетов по продажам.
		ПК-4.3	**Владее**т навыками построения прогнозов по продажам инфокоммуникационных систем и/или их составляющих по результатам проведенных исследований.
ПК-5	***Способен подготавливать расчетную и проектную документацию при разработке сетей, сооружений, средств и средств инфокоммуникаций***	**ПК-5.1**	**Знает** принципы построения технического задания при автоматизации проектирования средств и сетей связи и их элементов; структуру и основы подготовки технической и проектной документации
		ПК-5.2	**Умеет** выявлять и анализировать преимущества и недостатки вариантов проектных решений, оценивать риски, связанные с реализацией проекта

		ПК-5.3	**Владеет** навыками разработки рабочей документации и навыками проектирования систем станций подвижной радиосвязи

2. УЧЕБНАЯ ПРОГРАММА

2.1. Цели дисциплины - ознакомление студентов с основными понятиями, характеристиками и определениями информационных систем и телекоммуникационных технологий, как наиболее распространенных и достаточно уязвимых объектов с точки зрения информационной безопасности. Изучение математического аппарата в области теории информации и различных методов криптографического закрытия информации и методов корректирующего кодирования, грамотного выбора паролей и способов постановки цифровой подписи.

Задача – ознакомление студентов с основными теоретическими, техническими и организационными аспектами использования информационных технологий, проблемой обеспечения помехоустойчивости и безопасности информационных систем, изучение различных угроз и методов защиты от них.

2.2. Трудоемкость дисциплины и виды учебной работы (в академических часах и зачетных единицах) ***(удалить строки, которые не будут применены в рамках дисциплины)***

Виды учебной работы	**Всего, в акад. часах**	**Распределение по семестрам**					
		_III__ сем	**_IV_ сем**	**_V _ сем**	**_VI сем**	**VII сем**	**VIII сем**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1. Общая трудоемкость изучения дисциплины по семестрам, в т. ч.:	**108**					**108**	
1.1. Аудиторные занятия, в т. ч.:	**86**					**86**	
1.1.1. Лекции	**34**					**34**	
1.1.2. Практические занятия, в т. ч.	**52**					**52**	

1.1.2.1. Решение задач	**52**					**52**	
1.1.2.2. Контрольные работы							
1.2. Самостоятельная работа, в т. ч.:	**22**					**22**	
1.2.1.1.Письменные домашние задания							
1.3. Консультации							
Итоговый контроль (Экзамен, Зачет, диф. зачет - указать)						**Зачет**	

2.3. Содержание дисциплины

2.3.1. Тематический план и трудоемкость аудиторных занятий (модули, разделы дисциплины и виды занятий) по рабочему учебному плану

Разделы и темы дисциплины	**Всего (ак. часов)**	**Лекции (ак. часов)**	**Практ. Занятия (ак. часов)**	**Семинары (ак. часов)**	**Лабор. (ак. часов)**
1	**2=3+4+5+6**	**3**	**4**	**5**	**6**
МОДУЛЬ 1.БАЗОВЫЕ ПОНЯТИЯ ТЕОРИИ ИНФОРМАЦИИ	**9**	**4**	**5**		
Введение	**1**	**1**			
Раздел 1. Информация, ее виды и формы представления	**8**	**3**	**5**		
Тема 1.1.Виды информации и способы ее представления в информационных системах, структурная схема системы передачи цифровой информации	**3**	**1**	**2**		
Тема 1.2. Фазы обращения информации	**2**	**1**	**1**		
Тема 1.3. Способы измерения информации	**3**	**1**	**2**		

МОДУЛЬ 2. ОПРЕДЕЛЕНИЕ КОЛИЧЕСТВА ИНФОРМАЦИИ	**10**	**4**	**6**		
Раздел 5.Передача сообщений при наличии помех	**3**	**2**	**1**		
Тема 5.1. Пропускная способность канала связи при наличии помех, важнейшие классы помехоустойчивых кодов	**3**	**2**	**1**		
характеристики информации	**3**	**1**	**2**		
Раздел 3.Измерение информации	**4**	**2**	**2**		
Тема 3.1.Определение и свойства информации	**2**	**1**	**1**		
Тема 3.2. Передача информации от дискретного источника	**2**	**1**	**1**		

МОДУЛЬ 3. КОДЫ И ИХ ПРИМЕНЕНИЕ В СИСТЕМАХ ПЕРЕДАЧИ ИНФОРМАЦИИ	**10**	**4**	**6**		
Раздел 4.Эффективное кодирование для канала без помех	**7**	**2**	**5**		
Тема 4.1. Информационная избыточность сообщений	**3**	**1**	**2**		
Тема 4.2. Алфавитное неравномерное двоичное кодирование	**4**	**1**	**3**		

МОДУЛЬ 4. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ	**11**	**7**	**4**		
Раздел 6. Проблемы и задачи информационной безопасности	**5**	**3**	**2**		
Тема 6.1. Основные понятия и составляющие информационной безопасности	**1**	**1**			
Тема 6.2. Обеспечение информационной безопасности мобильных устройств	**1**	**1**			
Тема 6.3. Методы аутентификации пользователей инфокоммуникационной системы	**3**	**1**	**2**	**-**	
Раздел 7. Информационная безопасность инфокоммуникацонных систем и сетей	**6**	**4**	**2**		
Тема 7.1.Вредоносные программы и защита от них	**2**	**1**	**1**		
Тема 7.2. Аудит безопасности в инфокоммуникационных системах	**1**	**1**			
Тема 7.3.Предотвращение утечек информации в телекоммуникационных системах	**3**	**2**	**1**		

МОДУЛЬ 5. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ	**22**	**10**	**12**		
Раздел 8. Криптографическое закрытие информации	**15**	**7**	**8**		
Тема 8.1.Основные определения и терминология криптографии	**1**	**1**			
Тема 8.2. Классические шифры	**4**	**2**	**2**		
Тема 8.3. Симметричные криптосистемы	**5**	**2**	**3**		
Тема 8.4. Криптография открытого ключа	**5**	**2**	**3**		
Раздел 9.Контроль целостности данных	**7**	**3**	**4**		
Тема9.1. Электронная цифровая подпись	**4**	**2**	**2**		
Тема 9.2. Стеганография и стегоанализ	**3**	**1**	**2**		
МОДУЛЬ 6. БАЗОВЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ ДАННЫХ В СИСТЕМАХ МОБИЛЬНОЙ СВЯЗИ И ЭЛЕКТРОННОЙ ИДЕНТИФИКАЦИИ	**10**	**7**	**3**		
Раздел 10. Аспекты безопасности в системах подвижной радиосвязи	**6**	**4**	**2**		
Тема 10.1. Техническая безопасность в стандартах подвижной связи GSM и CDMA	**4**	**2**	**2**		
Тема 10.2. Техническая безопасность в стандартах подвижной связи LTE	**1**	**1**			
Тема 10.3.Информационная безопасность локальных беспроводных сетей стандарта IEEE 802.11	**1**	**1**			
Раздел 11. Обеспечение информационной безопасности систем электронной идентификации	**2**	**1**	**1**		
Тема 11.1. Обеспечение безопасности данных в системах RFID	**2**	**1**	**1**		

Раздел 12.Средства, системы и технические каналы утечки информации для осуществления киберслежки	**2**	**2**			
Тема 12.1. Средства, технологии и системы получения информативных признаков человека без применения технических средств разведки	**1**	**1**			
Тема 12.2. Средства и технологии скрытого получения информативных признаков человека через технические каналы утечки информации	**1**	**1**			
ИТОГО:	**86**	**34**		**52**	

2.3.2. Краткое содержание разделов дисциплины в виде тематического плана

МОДУЛЬ 1. БАЗОВЫЕ ПОНЯТИЯ ТЕОРИИ ИНФОРМАЦИИ

Введение

Краткая историческая справка о развитии теории информации. .Постановка проблемы безопасности инфокоммуникационных систем. Основные понятия теории вероятностей. Некоторые законы распределения случайных величин. Содержание дисциплины[1,4].

Раздел 1. Информация, ее виды и формы представления

Тема 1.1. Виды информации и способы ее представления в информационных системах, структурная схема системы передачи цифровой информации

Подходы к определению понятия «информация». Классификация информации по способу восприятия и форме представления. Сигнал, канал связи, сообщение, данные. Источник информации, приемник информации [1, Гл.1].

Тема 1.2. Фазы обращения информации

Принципы хранения, измерения, обработки и передачи информации. Меры количества и качества информации, [1, Гл.1].

Тема 1.3. Способы измерения информации

Измерение количества информации, единицы измерения информации. Передача информации, скорость передачи информации[1, Гл.1].

МОДУЛЬ 2. ОПРЕДЕЛЕНИЕ КОЛИЧЕСТВА ИНФОРМАЦИИ

Раздел 2. Энтропия, как мера степени неопределенности

Тема 2.1.Определение и свойства энтропии

Дискретный источник информации, мера неопределенности выбора состояния источника. Свойства энтропии. Энтропия сложной системы. Условная энтропия[1, Гл.6; 2, Гл.1].

Тема 2.2. Энтропия непрерывного источника информации

Относительная дифференциальная энтропия непрерывного источника информации. Условная энтропия, относительная дифференциальная условная энтропия непрерывного источника [3, Гл.8]

Раздел 3.Измерение информации

Тема 3.1.Определение и свойства информации

Общие понятия. Количество информации по Хартли и Шеннону. Объем информации. Взаимная информация [1, Гл. 6; 3, Гл. 4]

Тема 3.2. Передача информации от дискретного источника

Марковские и эргодические источники. Каналы связи. Количество информации, передаваемой по дискретному каналу[1, Гл.7]

МОДУЛЬ 3. КОДЫ И ИХ ПРИМЕНЕНИЕ В СИСТЕМАХ ПЕРЕДАЧИ ИНФОРМАЦИИ

Раздел 4.Эффективное кодирование для канала без помех

Тема 4.1. Информационная избыточность сообщений

Процесс передачи сообщения от источника к приемнику при отсутствии помех. Идеальный канал связи. Первичный алфавит, вторичный алфавит. Кодирование, декодирование. Информационная избыточность, полная информационная избыточность. Теорема Шеннона об источниках [3, Гл. 3; 1, Гл.7].

Тема 4.3. Алфавитное неравномерное двоичное кодирование

Принципы неравномерного кодирования. Основы префиксного кода. Неравенство Крафта. Префиксный код Шеннона-Фано, префиксный код Хаффмана [2, Гл. 2].

Раздел 5.Передача сообщений при наличии помех

Тема 5.1. Пропускная способность канала связи при наличии помех, структурная схема системы передачи цифровой информации

Математическое описание линии связи с помехами. Пропускная способность канала с помехами [3, Гл.8].Кодирование и декодирование информации блоковыми, циклическими и сверточными кодами [3, часть II, Гл.2-4].

МОДУЛЬ 4. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Раздел 6. Проблемы и задачи информационной безопасности

Тема 6.1. Основные понятия и составляющие информационной безопасности

Современное состояние, перспектива и ретроспектива. Информационные системы, средства, каналы, сети и среды. Основные понятия, определения и составляющие информационной безопасности. Наиболее опасные угрозы информационной безопасности. Информационные атаки. Технические каналы утечки информации. Основные задачи защиты информации [**9**, Гл.2].

Тема 6.2. Обеспечение информационной безопасности мобильных устройств

Модели использования мобильных устройств сотрудниками организации. Угрозы со стороны программного обеспечения. Сетевые и Интернет-угрозы. Угрозы физического доступа к устройству. Угрозы со стороны пользователей. Управление мобильными устройствами и приложениями [**10**, Гл.5].

Тема 6.3. Методы аутентификации пользователей инфокоммуникационной системы

Идентификация и аутентификация. Парольные системы аутентификации. Технологии единой аутентификации на нескольких Интернет-ресурсах. Биометрическая аутентификация. [**10**, Гл.3].

Раздел 7. Информационная безопасность компьютерных сетей

Тема 7.1.Вредоносные программы и защита от них

Классификация вредоносного программного обеспечения. Антивирусные программы [**9**, Гл.3].

Тема 7.2. Аудит безопасности в инфокоммуникационных системах

Управление рисками и инцидентами информационной безопасности. Организация центра управления событиями информационной безопасности (SOC). Базовые компоненты SOC. Основные механизмы функционирования SIEM-системы. [**10**, Гл.2].

Тема 7.3.Предотвращение утечек информации в телекоммуникационных системах

Прицнип работы **DLP(Data Leak Preventation) -** систем. Обзор интеллектуальной DLP-системы **InfoWatch Traffic Monitor [10,** Гл.7]

МОДУЛЬ 5. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Раздел 8. Криптографическое закрытие информации

Тема 8.1. Основные определения и терминология криптографии

Предмет и задачи криптографии и криптоанализа. История развития криптографии. Стойкость криптографического алгоритма. Основные требования, предъявляемые к методам шифрования информации. Классификация криптографических алгоритмов[**5**, Гл.1].

Тема 8.2. Классические шифры

Классические шифры перестановки: шифр «скитала», решетка Кардано. Шифры простой замены: квадрат Полибия, шифрующая система Цезаря. Криптоанализ шифров простой замены, гистограмма текста. Таблица Вижинера. Шифр Плейфера. Одноразовый шифровальный блокнот. Многоалфавитные методы шифрования. Шифры колонной замены. Шифровальные машины «Энигма» и «Лоренц» [**5**, Гл.1].

Тема 8.3. Симметричные криптосистемы

Способы построения вычислительно стойких блоковых шифров их криптоанализ. Композиции шифров. Схема Фейстеля. Алгоритм шифрования DES, основные режимы работы. Шифр AES. Вычислительная стойкость криптоалгоритмов. Атаки на алгоритмы шифрования. Основные методы криптоанализа блоковых шифров. Модификации блоковых шифров. Многократное шифрование. Требования, предъявляемые к современным блочным алгоритмам шифрования. Основные способы криптоанализа потоковых шифров . Генерация, распределение и хранение ключей шифрования для симметричных систем. Генераторы случайных и псевдослучайных чисел [**4**, Гл. 12, **5**, Гл.2].

Тема 8.4. Криптография открытого ключа

Ассиметричные системы шифрования, их особенности, преимущества и недостатки. Сравнение с симметричными системами. Протокол распределения ключей Диффи-Хеллмана,

стойкость протокола Диффи-Хелмана. Математический базис криптографии с открытым ключом. Шифр Шамира. Шифр Эль-Гамаля. Шифр RSA. Выбор параметров для криптосистемы RSA. Побочные атаки на алгоритм RSA. Физические атаки на криптоалгоритм RSA [**4**, Гл.11, **5**, Гл.3].

Раздел 9. Контроль целостности данных

Тема 9.1. Электронная цифровая подпись

Целостность данных. Функции хэширования. Бесключевые хеш-функции Основные требования к криптографическим хэш-функциям. Общие положения электронной цифровой подписи (ЭЦП). Основные требования, предъявляемые к схемам ЭЦП. Примеры электронной цифровой подписи на основе алгоритмов с открытыми ключами. Обзор основных криптографических протоколов [**5**, Гл.3].

Тема 9.2. Стеганография и стегоанализ

Структура, особенности построения и использования стеганографических систем. Терминология, сущность и цели стеганографического преобразования информации. Методы компьютерной стеганографии. Основные направления использования стеганографических систем. Основные принципы стеганографического анализа [**12**, Гл.1, Гл.4].

МОДУЛЬ 6. БАЗОВЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ ДАННЫХ В СИСТЕМАХ МОБИЛЬНОЙ СВЯЗИ И ЭЛЕКТРОННОЙ ИДЕНТИФИКАЦИИ

Раздел 10. Аспекты безопасности в системах подвижной радиосвязи

Тема 10.1. Техническая безопасность в стандартах подвижной связи GSM и CDMA

Угрозы сообщению. Угрозы пользователю. Угрозы системе. Пример практически используемых в стандарте GSM потоковых шифров A5/1…A5/3. Иерархия ключей, процедуры безопасности и шифрования в сети UTRAN. Механизмы обеспечения безопасности в стандарте CDMA 2000 [**6**, Гл.11, Гл.13]

Тема 10.2. Техническая безопасность в стандарте подвижной связи LTE

Алгоритмы шифрования, идентификации и аутентификации в стандарте LTE [**6**, Гл.13]

Тема 10.3 .Информационная безопасность локальных беспроводных сетей стандарта IEEE 802.11

Протоколы безопасности WEP, WPA и TKIP. Стандарты WPA2 и WPA3. Протокол IEEE 802.1X. Основные особенности и уязвимости протокола RADIUS. Сравнение технологий защиты беспроводных сетей стандарта 802.11 [**11**, Гл. 5]

Раздел 11. Обеспечение информационной безопасности систем электронной идентификации

Тема 11.1. Обеспечение безопасности данных в системах RFID

Обеспечение целостности и конфиденциальности передаваемых данных. Взаимная аутентификация ридера и транспондера [**7**, Гл.12].

Раздел 12. Специальные средства защиты

Тема 12.1.Средства, технологии и системы получения информативных признаков человека без применения технических средств разведки

Спутниковые, сотовые и радиотелефоны как устройства получения информативных признаков человека. Системы видеонаблюдения, спутникового и кабельного телевещания как средство получения информативных признаков людей [**8**, Гл.1].

Тема 12.2. Средства и технологии скрытого получения информативных признаков человека через технические каналы утечки информации

Общие понятия о технических каналах утечки информации, внутренние и внешние источники киберслежки [**8**, Гл.3].

2.3.3. Краткое содержание практических занятий-36 часов

1. Способы хранения, обработки и передачи информации
2. Единицы измерения информации
3. Носители информации
4. Определение объема данных в двоичной и десятичной системах счисления
5. Оценка условной энтропии ансамбля сообщений
6. Физическая сущность условной энтропии
7. Энтропия сложной системы
8. Поиск энтропии случайных величин.
9. Определение количества информации в равновероятном и не равновероятном сообщении
10. Взаимная информация

11. Определение скорости передачи информации
12. Скорость передачи информации при испольовании кода Бодо
13. Основы кодирования сообщений: первичный и вторичный алфавиты, оптимальный код
14. Общая и частная избыточности алфавита
15. Избыточность сообщений при побуквенном и блочном кодировании
16. Алфавитное кодирование с неравной длительностью сигналов
17. Принципы неравномерного кодирования
18. Основы префиксного кода
19. Установление связи средней длины кода с энтропией
20. Кодирование по методу Шеннона-Фано
21. Кодирование по методу Хаффмана
22. Исследование алгоритма Лемпеля — Зива
23. Установление связи ширины полосы канала со скоростью передачи информации
24. Основная теорема Шеннона о кодировании для канала с помехами
25. Линейные блоковые коды: построение и основные свойства. Порождающая и проверочные матрицы систематического линейного кода
26. Коды Хемминга: процедуры кодирования и декодирования
27. Код Боуза-Чоудхури-Хоквингема и Рида-Соломона
28. Кодирование информации сверточными кодами
29. Программно-аппаратные средства обеспечения информационной безопасности в компьютерных сетях
30. Применение антивирусных сканеров Dr.Web CureIt и Kaspersky Virus Removal Tool для защита программного обеспечения от вирусного заражения, разрушающих программных действий и изменений
31. Защита и генерация стойких паролей посредством менеджеров паролей LastPass, KeePas, Google Password Manager и Kaspersky Password Manager
32. Тестирование fingerprint- и face ID- сканеров мобильных устройств
33. Блокировка файловых операций по результатам лингвистического анализа содержания файлов между компьютером и съёмными носителями посредством InfoWatch Traffic Monitor

34. Настройка политики запрета на снятие снимков экрана из Excel и Word в модуле InfoWatch Device Monitor
35. Использование классических криптоалгоритмов перестановки и подстановки для защиты текстовой информации
36. Изучение устройства и принципа работы шифровальной машины «Энигма»
37. Шифры гаммирования
38. Результаты теории информации для криптографии, теорема Шеннона
39. Дешифрование шифра простой перестановки при помощи метода биграмм
40. Схема Фейстеля
41. Стандарт симметричного шифрования DES
42. Генерация псевдослучайных чисел методом Блюм-Блюма-Шуба
43. Понятие односторонней функции. Использование односторонних функций в криптографических алгоритмах
44. Система Диффи-Хеллмана
45. Математическая база асимметричной криптографии: фунцкия Эйлера, малая теорема Ферма, теорема Эйлера, расширенный алгоритм Евклида, алогоритм повторного умножения по модулю, алгоритм повторного возведения в квадрат по модулю
46. Генерация простых чисел, используемых в асимметричных системах шифрования
47. Шифр Шамира
48. Шифр Эль-Гамаля
49. Алгоритм RSA
50. Безопасность алгоритма RSA и виды основных атак
51. Электронная цифровая подпись на основе RSA
52. Электронная цифровая подпись на основе схемы Эль-Гамаля
53. Применение стегокомплекса Invisible Secrets-4
54. Применение криптографических алгоритмовA3, A8 и A5
55. Взаимная аутентификация с использованием секретного криптоключа
56. Взаимная аутентификация с использованием выведенных криптоключей

2.3.4. Материально-техническое обеспечение дисциплины

(Кратко представить перечень материально-технического оснащения, информационно-технических средств).

- Учебные методические пособия,
- мультимедийная аудитория с широкополосным доступом в сеть интернет,
- персональный компьютер,
- доска и маркер,
- проектор.

2.4. Модульная структура дисциплины с распределением весов по формам контролей

Формы контролей	Вес формы (форм) текущего контроля в результирующей оценке текущего контроля (по модулям)		Вес формы промежуточного контроля в итоговой оценке промежуточного контроля		Вес итоговой оценки промежуточного контроля в результирующей оценке промежуточных контролей		Вес итоговой оценки промежуточного контроля в результирующей оценке промежуточных контролей (семестровой оценке)	Веса результирующей оценки промежуточных контролей и оценки итогового контроля в результирующей оценке итогового контроля
Вид учебной работы/контроля	**М1**[1]	**М2**	**М1**	**М2**	**М1**	**М2**		
Контрольная работа *(при наличии)*				1				
Устный опрос *(при наличии)*								
Тест *(при наличии)*								
Лабораторные работы *(при наличии)*								
Письменные домашние задания *(при наличии)*								
Реферат *(при наличии)*								
Эссе *(при наличии)*								
Проект *(при наличии)*								
Решение задач		1						
Веса результирующих оценок текущих контролей в итоговых оценках промежуточных						0,5		

[1] Учебный Модуль

контролей								
Веса оценок промежуточных контролей в итоговых оценках промежуточных контролей						0,5		
Вес итоговой оценки 1-го промежуточного контроля в результирующей оценке промежуточных контролей								
Вес итоговой оценки 2-го промежуточного контроля в результирующей оценке промежуточных контролей							1	
Вес результирующей оценки промежуточных контролей в результирующей оценке итогового контроля								0,4
Вес итогового контроля (Экзамен/зачет) в результирующей оценке итогового контроля								0,6
	∑ = 1	**∑ = 1**	**∑ = 1**	**∑ = 1**	**∑ = 1**	**∑ = 1**	**∑ = 1**	**∑ = 1**

3. **Теоретический блок** ***(указываются материалы, необходимые для освоения учебной программы дисциплины)***

3.1. Материалы по теоретической части курса

3.1.1. Учебник(и);

3.1.2. Учебное(ые) пособие(я);

Основная литература

1. **Костров Б.В.** Основы цифровой передачи и кодирования информации.-М.: «ТехБук», 2007.-192 с.
2. **Кудряшов Б.Д.** Теория информации:Учебник для вузов.-СПб.:Питер, 2009.- 320 с.
3. **Вернер М.** Основы кодирования: Учебник для ВУЗов.-М.: Техносфера, 2004.-288с.
4. **Макаренко С. И.** Информационная безопасность: учебное пособие для студентов вузов. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.: ил.
5. **Васильева И.Н.** Криптографические методы защиты информации: учебник и практикум для академического бакалавриата.-М.: Издательство Юрайт, 2017.-349 с.

6. **Бабков В.Ю., Цикин И.А.** Сотовые системы мобильной радиосвязи: учеб. пособие.-2-е изд., перераб. и доп.-СПб.:БХВ-Петербург, 2013.-432 с.

Дополнительная литература:

7. **Дшхунян В.Л., Шаньгин В.Ф.** Электронная идентификация. Бесконтактные идентификаторы и смарт-карты.- М.: «Издательство АСТ»: Издательство «НТ Пресс», 2004.-695 с.
8. **Технические средства и методы защиты информации: Учебник для вузов** / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство Машиностроение», 2009 – 508 с.
9. **Баранова Е.К., Бабаш А.В.** Основы информационной безопасности: учебник.- М.:РИОР: ИНФРА-М, 2019.-202 с.
10. **Карпухин Е.О.** Технологии и методы защиты инфокоммуникационных систем и сетей.Учебное пособие для вузов.-М.: Горячая линия-Телеком, 2020.-120 с.
11. **Вишневский В.М., Портной С.Л., Шахнович И.В.** Энциклопедия WiMAX: Путь к 4G.- М.:Техносфера, 2009.-472 с.
12. **Федосеев В.А.** Теоретические основы стеганографии и цифровых водяных знаков: учеб. пособие.- Самара: Самарский университет, 2017.-132 с.

3.1.3. Электронные материалы (электронные учебники, учебные пособия, курсы и краткие конспекты лекций, презентации PPT и т.п.);

4. Фонды оценочных средств ***(указываются материалы, необходимые для проверки уровня знаний в соответствии с содержанием учебной программы дисциплины).***

4.1. Перечень вопросов для итогового контроля

1. Подходы к определению понятия «информация»
2. Классификация информации по способу восприятия и форме представления.
3. Сигнал, канал связи, сообщение, данные. Источник информации, приемник информации
4. Принципы хранения, измерения, обработки и передачи информации
5. Меры количества и качества информации
6. Измерение количества информации, единицы измерения информации
7. Передача информации, скорость передачи информации
8. Дискретный источник информации, мера неопределенности выбора состояния источника.
9. Свойства энтропии. Энтропия сложной системы, условная энтропия
10. Относительная дифференциальная энтропия непрерывного источника информации

11. Условная энтропия, относительная дифференциальная условная энтропия непрерывного источника
12. Количество информации по Хартли и Шеннону, объем информации, взаимная информация
13. Марковские и эргодические источники. Каналы связи
14. Количество информации, передаваемой по дискретному каналу
15. Процесс передачи сообщения от источника к приемнику при отсутствии помех
16. Идеальный канал связи. Первичный алфавит, вторичный алфавит. Кодирование, декодирование
17. Информационная избыточность
18. Неравенство Крафта
19. Теорема Шеннона об источниках
20. Принципы неравномерного кодирования.
21. Основы префиксного кода. Префиксный код Шеннона-Фано, префиксный код Хаффмана
22. Математическое описание линии связи с помехами. Пропускная способность канала с помехами
23. Порождающая и проверочная матрица систематического линейного кода
24. Конечные поля. Арифметика полей Галуа
25. Порождающий и проверочный многочлены циклического кода
26. Декодирование кодов БЧХ поформулам
27. Декодирование кодов БЧХ алгоритмом ПГЦ
28. Кодирование и декодирование информации кодами Рида-Соломона
29. Кодирование и декодирование информации сверточными кодами
30. Основные понятия, определения и составляющие информационной безопасности
31. Наиболее опасные угрозы информационной безопасности
32. Информационные атаки. Технические каналы утечки информации
33. Модели использования мобильных устройств сотрудниками организации.
34. Угрозы со стороны программного обеспечения. Сетевые и Интернет-угрозы. Угрозы физического доступа к устройству. Угрозы со стороны пользователей.
35. Управление мобильными устройствами и приложениями
36. Идентификация и аутентификация. Парольные системы аутентификации. Технологии единой аутентификации на нескольких Интернет-ресурсах

37. Биометрическая аутентификация
38. Классификация вредоносного программного обеспечения. Антивирусные программы
39. Управление рисками и инцидентами информационной безопасности
40. Организация центра управления событиями информационной безопасности (SOC). Базовые компоненты SOC
41. Основные механизмы функционирования SIEM-системы
42. Принцип работы DLP(Data Leak Preventation) - систем
43. Предмет и задачи криптографии и криптоанализа. История развития криптографии.
44. Стойкость криптографического алгоритма. Классификация криптографических алгоритмов
45. Классические шифры перестановки: шифр «скитала», решетка Кардано. Шифры простой замены: квадрат Полибия, шифрующая система Цезаря. Криптоанализ шифров простой замены, гистограмма текста.
46. Таблица Вижинера. Шифр Плейфера. Одноразовый шифровальный блокнот. Многоалфавитные методы шифрования. Шифры колонной замены. Шифровальные машины «Энигма» и «Лоренц»
47. Способы построения вычислительно стойких блоковых шифров их криптоанализ. Композиции шифров. Схема Фейстеля.
48. Алгоритм шифрования DES, основные режимы работы
49. Шифр AES
50. Вычислительная стойкость криптоалгоритмов. Атаки на алгоритмы шифрования
51. Основные методы криптоанализа блоковых шифров. Модификации блоковых шифров. Многократное шифрование.
52. Требования, предъявляемые к современным блочным алгоритмам шифрования.
53. Основные способы криптоанализа потоковых шифров.
54. Генерация, распределение и хранение ключей шифрования для симметричных систем. Генераторы случайных и псевдослучайных чисел
55. Ассиметричные системы шифрования, их особенности, преимущества и недостатки. Сравнение с симметричными системами
56. Протокол распределения ключей Диффи-Хеллмана, стойкость протокола Диффи-Хелмана
57. Математические основы асимметричной криптографии.
58. Шифр Шамира. Шифр Эль-Гамаля

59. Шифр RSA. Выбор параметров для криптосистемы RSA.
60. Побочные атаки на алгоритм RSA. Физические атаки на криптоалгоритм RSA.
61. Целостность данных. Функции хэширования. Бесключевые хеш-функции. Основные требования к криптографическим хэш-функциям
62. Общие положения электронной цифровой подписи (ЭЦП). Основные требования, предъявляемые к схемам ЭЦП. Примеры электронной цифровой подписи на основе алгоритмов с открытыми ключами.
63. Обзор основных криптографических протоколов
64. Структура, особенности построения и использования стеганографических систем. Терминология, сущность и цели стеганографического преобразования информации.
65. Методы компьютерной стеганографии. Основные направления использования стеганографических систем. Основные принципы стеганографического анализа
66. Угрозы сообщению. Угрозы пользователю. Угрозы системе
67. Пример практически используемых в стандарте GSM потоковых шифров A5/1…A5/3
68. Иерархия ключей, процедуры безопасности и шифрования в сети UTRAN
69. Механизмы обеспечения безопасности в стандарте CDMA 2000
70. Алгоритмы шифрования, идентификации и аутентификации в стандарте LTE
71. Протоколы безопасности WEP, WPA и TKIP
72. Стандарты WPA2 и WPA3
73. Протокол IEEE 802.1X. Основные особенности и уязвимости протокола RADIUS. Сравнение технологий защиты беспроводных сетей стандарта 802.11
74. Обеспечение целостности и конфиденциальности передаваемых данных. Взаимная аутентификация ридера и транспондера
75. Основные средства и технологии получения информативных признаков человека
76. Средства выявления технических каналов утечки информации

4.2. Образец варианта теста итогового контроля

Билет № 5

ФИО студента

1. **При кодировании методом Хаффмана на 0 и на 1 придется тратить:**

   a. не менее одного байта,
   b. максимум один бит,

c. не менее одного бита,
d. максимум один килобайт.

2. **Кодирование представляет собой:**

a. преобразование аналоговой информации,
b. искусственное создание помех в канале связи при передаче информации,
c. преобразование дискретной информации,
d. процесс зашифрования информации.

3. **При неравномерном экономном кодировании (например, методом Хаффмена или Шеннона-Фано) для отображения наиболее вероятных символов используется _____ количество разрядов:**

a. максимальное,
b. минимальное,
c. среднее (среднее арифметическое),
d. среднее (среднее геометрическое).

4. **Если у кода $d_{min} = 1$, то:**

a. все кодовые комбинации являются разрешенными,
b. все кодовые комбинации являются запрещенными,
c. применяется декодирование по методу максимального правдоподобия,
d. любая одиночная ошибка трансформирует данную комбинацию в запрещенную.

5. **Экономное кодирование абсолютно неэффективно, если вероятности появления символов алфавита источника подчиняются _____ закону распределения:**

a. нормальному,
b. равномерному,
c. биномиальному,
d. релеевскому.

6. **Угроза информационной безопасности-это:**

a. чтение, обновление или разрушение информации при отсутствии на это соответствующих полномочий;
b. незаконное подключение к линиям связи;
c. совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения информационной безопасности;
d. дистанционное преодоление систем защиты.

7. **Классификация компьютерных вирусов по особенностям реализуемого алгоритма:**

a. файловые вирусы, загрузочные вирусы, комбинированные вирусы;
b. активные, пассивные;
c. разидентные, нерезидентные;
d. безвредные, неопасные, опасные и очень опасные вирусы;

e. вирусы-спутники, паразитические вирусы, стелс-вирусы (вирусы-невидимки), полиморфные вирусы (вирусы-призраки).

8. Подберите слово к данному определению:

_____ - это достаточно трудно обнаружимые вирусы, не имеющие сигнатур, т.е. не содержащие ни одного постоянного участка кода.

a. полиморфик-вирусы;
b. стелс-вирусы;
c. макровирусы;
d. конструкторы вирусов**.**

9. Аутентификация-это:

a. проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности;

b. присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным;

c. гарантирование того, что информация остается неизменной, корректной и аутентичной.

d. гарантирование того, что авторизированные пользователи могут иметь доступ и работать с информационными активами, ресурсами и системами, которые им необходимы, при этом обеспечивается требуемая производительность.

10. Для шифрования данных в системах сотовой связи стандарта GSM используется алгоритм шифрования:

a. с открытым ключом A5;
b. с секретным ключом A5;
c. с октрытым ключом A8;
d. с секретным ключом A3.