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.07 «Криптография и безопасность»

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

Направление подготовки: 11.04.02 Инфокоммуникационные технологии и системы связи

Наименование образовательной программы: «Беспроводные коммуникации и сенсоры»

1. АННОТАЦИЯ

1.1. Краткое описание содержания данной дисциплины;

В курсе дисциплины “Криптография и безопасность” излагаются основные понятия криптографических методов и средств защиты информации, необходимые для профессиональной деятельности в области информационных технологий и систем связи. Рассматриваются общие характеристики методов криптографической защиты информации, приводятся описание средств, принципов и механизмов обеспечения информационной безопасности и средств защиты компьютерной информации с применением криптографии. Даны определения и примеры криптографического закрытия информации. Подробно рассмотрены классические и современные симметричные и асимметричные криптосистемы шифрования, методы создания цифровой подписи, специальные технические средства для защиты помещений и аппаратуры. Описываются процедуры аутентификации и шифрования в системах радиочастотной идентификации и мобильной радиосвязи разных поколений.

1.2. Трудоемкость в академических кредитах - 2, в часах -72, форма итогового контроля - зачет;

1.3. Данная дисциплина теснейшим образом связана со следующими дисциплинами: цифровая связь, вероятность и случайные процессы, линейная алгебра и приложения, введение в цифровую обработку сигналов, теория кодирования и сжатие данных

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)*
ПК-4	***Способен обеспечивать информационную безопасность системного программного обеспечения инфокоммуникационной системы ПГУ***	***ПК-4.1***	**Знает** основы обеспечения информационной безопасности, нормативные правовые акты в области информационной безопасности, системное программное обеспечение.

		ПК-4.2	**Умеет** осуществлять сбор и анализ исходных данных для обеспечения информационной безопасности системного программного обеспечения.
		ПК-4.3	**Владеет** навыками установки и настройки аппаратно - программных средств защиты системного программного обеспечения.
ПК-5	***Способен организовывать и проводить экспериментальные испытания с целью оценки и улучшения качества предоставляемых услуг связи, соответствия требованиям технических регламентов, международных и национальных стандартов и иных нормативных документов***	***ПК-5.1***	**Знает** основы архитектуры, устройства и функционирования вычислительных систем, стандарты информационного взаимодействия систем.
		ПК-5.2	**Умеет** собирать данные для анализа показателей качества программных технических средств инфокоммуникационной системы и анализировать системные проблемы обработки системы.
		ПК-5.3	**Владеет** навыками обнаружения и определения причин возникновения критических инцидентов при работе системного программного обеспечения.
ПК-6	***Способен проводить инсталляцию, настройку и обслуживание программного обеспечения телекоммуникационного***	***ПК-6.1***	**Знает** основы электротехники, принципы построения и функционирования сетей связи, основы сетевых технологий

	оборудования		
		ПК-6.2	**Умеет** устанавливать и настраивать программное обеспечение, диагностировать работу сетевого оборудования, выявлять проблемы и находить решения.
		ПК-6.3	**Владеет** навыками установки и настройки программного обеспечения телекоммуникационного оборудования системами мониторинга и контроля работоспособности сетевых сервисов и телефонии.
ПК-7	***Способен к выполнению работ по обеспечению функционирования телекоммуникационного оборудования корпоративных сетей с учетом требований информационной безопасности***	***ПК-7.1***	**Знает** основы сетевых технологий, стандарты и методы защищенной передачи данных в корпоративных сетях современные технологии и стандарты администрирования телекоммуникационных корпоративных сетей.
		ПК-7.2	**Умеет** поддерживать актуальность сетевой инфраструктуры, вести электронные базы данных применять новые технологии администрирования, использовать средства диагностики и мониторинга оборудования.
		ПК-7.3	**Владеет** навыками администрирования системного и сетевого программного обеспечения,навыками защиты баз данных от несанкционированного доступа.

ПК-8	***Способен к администрированию системного программного обеспечения и систем управления базами данных инфокоммуникационной системы ПГУ***	***ПК-8.1***	**Знает** архитектуру программных компонентов СУБД и операционные системы.
		ПК-8.2	**Умеет** администрировать и архивировать базы данных, использовать современные программно-аппаратные средства резервирования данных, пользоваться нормативно-технической документацией по файловым системам.
		ПК-8.3	**Владеет** методами сжатия и хранения информации, способностью осуществлять самостоятельный поиск информации, необходимой для выполнения профессиональных задач и английским языком на уровне чтения технической документации.
ПК-9	***Способен к администрированию процесса поиска и диагностики ошибок сетевых устройств и программного обеспечения***	***ПК-9.1***	**Знает** общие принципы функционирования и архитектуру аппаратных, программных и программно-аппаратных средств администрируемой сети
		ПК-9.2	**Умеет** пользоваться контрольно-измерительными приборами и аппаратурой, анализировать сообщения об ошибках в сетевых устройствах и операционных системах.
		ПК-9.3	**Владеет** навыками мониторинга установленных сетевых устройств и

			программного обеспечения, выявления и устранения сбоев и отказов сетевых устройств.

2. УЧЕБНАЯ ПРОГРАММА

2.1. Цель дисциплины - ознакомление студентов с основными понятиями и определениями криптографии и информационной безопасности, необходимыми для профессиональной деятельности в области информационных технологий и телекоммуникаций. Изучение математического аппарата в области различных методов криптографического закрытия информации, грамотного выбора паролей и способов постановки цифровой подписи.

Задача - ознакомление студентов с основными понятиями криптографической защиты информации, проблемой обеспечения безопасности информационных систем, изучение различных угроз и методов защиты от них.

2.2. Трудоемкость дисциплины и виды учебной работы (в академических часах-72 и зачетных единицах -2) ***(удалить строки, которые не будут применены в рамках дисциплины)***

Виды учебной работы	Всего, в акад. часах	Распределение по семестрам					
		I сем	II сем	III сем	IV сем.	___ сем	____ сем.
1	2	3	4	5	6	7	8
1. Общая трудоемкость изучения дисциплины по семестрам, в т. ч.:	**72**			**72**			
1.1. Аудиторные занятия, в т. ч.:	**34**			**34**			
1.1.1. Лекции	**18**			**18**			
1.1.2. Практические занятия, в т. ч.							
1.1.2.1. Решение задач	**16**			**16**			
1.2. Самостоятельная работа, в т. ч.:	**38**			**38**			
1.2.1. Другие виды самостоятельной работы, в т.ч. (указать)							

1.2.1.1.Письменные домашние задания							
1.3. Консультации							
Итоговый контроль (Экзамен, Зачет, диф. зачет - указать)	**Зачет**			**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	**5**	**3**	**2**		
Введение	**1**	**1**			
Раздел 1. Информация, ее виды и формы представления	**3**	**2**	**1**		
Тема 1.1. Виды информации и способы ее представления в информационных системах	**1**	**1**			
Тема 1.2. Фазы обращения и способы измерения информации	**2**	**1**	**1**		
МОДУЛЬ 2. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА	**9**	**6**	**3**		

Раздел 2. Проблемы и задачи информационной безопасности	**3**	**3**			
Тема 2.1. Основ ные понятия и составляющие информационной безопасности	**1**	**1**			
Тема 2.2. Политика информационной безопасности	**1**	**1**			
Тема 2.3. Механизмы обеспечения информационной безопасности	**1**	**1**	**-**	**-**	
Раздел 3. Информационная безопасность компьютерных сетей	**5**	**2**	**3**	**-**	
Тема 3.1. Вредоносные программы и защита от них	**3**	**1**	**2**	**-**	
Тема 3.2. Особенности обеспечения информационной безопасности в компьютерных сетях	**2**	**1**	**1**	**-**	
МОДУЛЬ 3. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ	**18**	**9**	**9**		
Раздел 4. Криптографическое закрытие информации	**12**	**6**	**6**		
Тема 4.1. Предмет и задачи криптографии и криптоанализа	**1**	**1**			
Тема 4.2. Классические шифры	**3**	**1**	**2**		
Тема 4.3. Симметричные криптосистемы	**3**	**1**	**2**		
Тема 4.4. Асимметричные криптосистемы	**5**	**3**	**2**		
Раздел 5. Контроль целостности данных	**6**	**3**	**3**		
Тема 5.1. Электронная цифровая подпись	**3**	**1**	**2**		
Тема 5.2. Современные приложения криптографии	**3**	**2**	**1**	**-**	
МОДУЛЬ 4. БАЗОВЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ ДАННЫХ В СИСТЕМАХ МОБИЛЬНОЙ СВЯЗИ И ЭЛЕКТРОННОЙ ИДЕНТИФИКАЦИИ	**4**	**2**	**2**		
Раздел 6. Аспекты безопасности в сотовых системах подвижной радиосвязи	**2**	**1**	**1**	**-**	
Тема 6.1. Техническая безопасность в стандартах подвижной связи GSM, CDMA и LTE	**2**	**1**	**1**		

Раздел 7. Обеспечение информационной безопасности систем электронной идентификации	**2**	**1**	**1**		
Тема 7.1. Обеспечение безопасности данных в микропроцессорных картах и системах RFID	**2**	**1**	**1**		
ИТОГО:	**36**	**18**	**16**		

2.3.2. Краткое содержание разделов дисциплины в виде тематического плана

Введение

Краткая историческая справка о развитии теории информации. Постановка проблемы информационной безопасности. Основные понятия теории вероятностей. Некоторые законы распределения случайных величин. Содержание дисциплины [1,2].

Раздел 1. Информация, ее виды и формы представления

Тема 1.1. Виды информации и способы ее представления в информационных системах

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 и способы измерения информации

Принципы хранения, измерения, обработки и передачи информации. Меры количества и качества информации. Измерение количества информации, единицы измерения информации. Передача информации, скорость передачи информации [**1**, Гл.1].

МОДУЛЬ 2. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Раздел 2. Проблемы и задачи информационной безопасности

Тема 2.1. 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. Анализ угроз информационной безопасности, угрозы нарушения доступности, целостности и конфиденциальности информации. Технические каналы утечки информации. Основные задачи защиты информации [**2**, Гл.1].

Тема 2.2. Политика информационной безопасности

Задачи информационной безопасности общества. Уровни формирования режима информационной безопасности. Ответственность за нарушения в сфере информационной безопасности. Стандарты информационной безопасности. Административный уровень обеспечения информационной безопасности. Анализ и оценка рисков информационной безопасности [**2**, Гл.6, Гл.7, **7,** Гл.1].

Тема 2.3. Механизмы обеспечения информационной безопасности

Идентификация и аутентификация. Биометрическая аутентификация. Методы разграничения доступа. Регистрация и аудит. Технология виртуальных частных сетей [**2**, Гл.10; Гл.17, **7,** Гл.4].

Раздел 3. Информационная безопасность компьютерных сетей

Тема 3.1. Вредоносные программы и защита от них

Классификация вредоносного программного обеспечения. Антивирусные программы. Угрозы для мобильных устройств [**2**, Гл.13, 7, Гл.2].

Тема 3.2. Особенности обеспечения информационной безопасности в компьютерных сетях

Локальные и сетевые (удаленные) угрозы. Сетевые модели передачи данных. Модель взаимодействия открытых систем OSI/ISO. Стек протоколов TCP/IP. Классификация удаленных угроз в вычислительных сетях [**2**, Гл.15, **7**, Гл.4].

МОДУЛЬ 3. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Раздел 4. Криптографическое закрытие информации

Тема 4.1. Предмет и задачи криптографии и криптоанализа

Предмет и задачи криптографии и криптоанализа. История развития криптографии.Стойкость криптографического алгоритма. Классификация криптографических алгоритмов [**3**, Гл.1].

Тема 4.2. Классические шифры

Классические шифры перестановки: шифр «скитала», решетка Кардано и шифр Ришелье. Шифры простой замены: квадрат Полибия, шифрующая система Цезаря. Криптоанализ шифров простой замены. Таблица Тритемия, шифровальный диск Альберти. Шифр Вижинера. Шифр Вернама. Шифры колонной замены. Шифровальные машины [**3**, Гл.1, **6**, Ч.1].

Тема 4.3. Симметричные криптосистемы

Основы теории Шенонна и ее развитие. Модели шифров. Результаты теории информации для криптографии. Композиции шифров. Сеть Фейстеля. Алгоритм шифрования DES, основные режимы работы. Модификации алгоритма DES. Шифр AES. Вычислительная стойкость криптоалгоритмов. Атаки на алгоритмы шифрования. Методы криптоанализа блочных шифров. Требования, предъявляемые к современным блочным алгоритмам шифрования. Генерация, распределение и хранение ключей шифрования для симметричных систем. Генераторы случайных и псевдослучайных чисел [**3**, Гл.2, **6**, Ч.3].

Тема 4.4. Асимметричные криптосистемы

Ассиметричные системы шифрования, их особенности, преимущества и недостатки. Сравнение с симметричными системами. Система Диффи-Хеллмана. Математические основы асимметричной криптографии. Функции, используемые в криптографических системах, однонаправленные функции. Шифр Шамира. Шифр Эль-Гамаля. Шифр RSA. Атаки на алгоритм RSA. Гибридные криптосистемы [**3**, Гл.3, **6**, Ч.2].

Раздел 5. Контроль целостности данных

Тема 5.1. Электронная цифровая подпись

Целостность данных. Функции хэширования. Требования к хэш-функциям. Общие положения электронной цифровой подписи. Алгоритмы цифровой подписи RSA и DSA. Схема подписи Эль-Гамаля [**3**, Гл.3].

Тема 5.2. Современные приложения криптографии

Системы тайного электронного голосования. Электронные деньги. Электронная жеребьевка. Защита документов и ценных бумаг от подделки. Стеганографические методы защиты информации. Системы встраивания информации в изображения, видео и звуковые сигналы [**3**, Гл.3, **6**, Ч.4].

МОДУЛЬ 4. БАЗОВЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ ДАННЫХ В СИСТЕМАХ МОБИЛЬНОЙ СВЯЗИ И ЭЛЕКТРОННОЙ ИДЕНТИФИКАЦИИ

Раздел 6. Аспекты безопасности в сотовых системах подвижной радиосвязи

Тема 6.1. Техническая безопасность в стандартах подвижной связи GSM, CDMA и LTE

Угрозы сообщению. Угрозы пользователю. Угрозы системе. Протоколы шифрования/дешифрования в стандартах подвижной связи GSM, CDMA и LTE [**4**, Гл.11, Гл.13]

Раздел 7. Обеспечение информационной безопасности систем электронной идентификации

Тема 7.1. Обеспечение безопасности данных в микропроцессорных картах и системах RFID

Аутентификация, основанная на алгоритмах симметричного и асимметричного шифрования. Обеспечение целостности и конфиденциальности передаваемых данных. Взаимная аутентификация ридера и транспондера. Проблемы и особенности организации защиты смарт-карт [**5**, Гл. 11, 12].

2.3.3. Краткое содержание практических занятий – 16 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. Определение скорости передачи информации
6. Скорость передачи информации при испольвании кода Бодо
7. Программно-аппаратные средства обеспечения информационной безопасности в компьютерных сетях
8. Защита программного обеспечения от вирусного заражения, разрушающих программных действий и изменений
9. Особенности защиты информации в компьютерных сетях
10. Уровни сетевых атак согласно модели OSI
11. Виды атак на сетевые компоненты. Атаки на DNS- сервера
12. Использование классических криптоалгоритмов перестановки и подстановки для защиты текстовой информации
13. Имитостойкость и криптографическая стойкость
14. Способы скрытой передачи данных
15. Сокрытие информации в звуковых файлах формата MIDI и WAV
16. Применение стеганографических программ DeEgger Embedder,SilentEye и Xiao Steganography
17. Изучение устройства и принципа работы шифровальной машины «Энигма»
18. Шифры гаммирования

19. Результаты теории информации для криптографии, теорема Шеннона
20. Дешифрование шифра простой перестановки при помощи метода биграмм
21. Сеть Фейстеля
22. Стандарт симметричного шифрования DES
23. Генерация псевдослучайных чисел методом Блюм-Блюма-Шуба
24. Понятие односторонней функции. Использование односторонних функций в криптографических алгоритмах
25. Система Диффи-Хеллмана
26. Математические основы асимметричной криптографии: фунцкия Эйлера, малая теорема Ферма, теорема Эйлера, расширенный алгоритм Евклида,алогоритм повторного умножения по модулю, алгоритм повторного возведения в квадрат по модулю
27. Проверка чисел на простоту, тест Миллера-Рабина
28. Шифр Шамира
29. Шифр Эль-Гамаля
30. Алгоритм RSA
31. Безопасность алгоритма RSA и виды основных атак
32. Электронная цифровая подпись на основе RSA
33. Электронная цифровая подпись на основе схемы Эль-Гамаля
34. Скрытие речевой информации в телефонных системах с использованием криптографических методов
35. Применение криптографических алгоритмов A3, A8 и A5
36. Взаимная аутентификация с использованием секретного криптоключа
37. 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)*								
Устный опрос *(при наличии)*								
Тест *(при наличии)*								
Лабораторные работы *(при наличии)*								
Письменные домашние задания *(при наличии)*				1				
Реферат *(при наличии)*								
Эссе *(при наличии)*								
Проект *(при наличии)*								
Решение задач	1							
Веса результирующих оценок текущих контролей в итоговых оценках промежуточных контролей						0.5		
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							1	

[1] Учебный Модуль

промежуточных контролей								
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. **Макаренко С. И.** Информационная безопасность: учебное пособие для студентов вузов. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.: ил.
3. **Васильева И. Н.** Криптографические методы защиты информации: учебник и практикум для академического бакалавриата.-М.: Издательство Юрайт, 2017.-349 с.

Дополнительная литература:

4. **Бабков В. Ю., Цикин И. А.** Сотовые системы мобильной радиосвязи: учеб. пособие.- 2-е изд., перераб. и доп.-СПб.:БХВ-Петербург, 2013.- 432 с.
5. **Дшхунян В. Л., Шаньгин В. Ф.** Электронная идентификация. Бесконтактные идентификаторы и смарт-карты.- М.: «Издательство АСТ»: Издательство «НТ Пресс», 2004.-695 с.
6. **Баранова Е. К.** Криптографические методы защиты информации. Лабораторный практикум: учебное пособие / Е.К. Баранова, А.В.Бабаш .- М.: КНОРУС, 2015.- 200 с.

7. **Баранова Е.К.** Информационная безопасность и защита информации:учебное пособие/ Е.К. Баранова, А.В. бабаш.-М.:ЕАОИ, 20212.-311.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

5. Подходы к определению понятия «информация»
6. Классификация информации по способу восприятия и форме представления.
7. Сигнал, канал связи, сообщение, данные. Источник информации, приемник информации
8. Принципы хранения, измерения, обработки и передачи информации
9. Меры количества и качества информации
10. Измерение количества информации, единицы измерения информации
11. Передача информации, скорость передачи информации
12. Основные понятия, определения и составляющие информационной безопасности
13. Наиболее опасные угрозы информационной безопасности
14. Информационные атаки. Технические каналы утечки информации
15. Уровни формирования режима информационной безопасности.
16. Стандарты информационной безопасности.
17. Административный уровень обеспечения информационной безопасности
18. Анализ и оценка рисков информационной безопасности
19. Идентификация и аутентификация. Биометрическая аутентификация
20. Методы разграничения доступа. Регистрация и аудит
21. Технология виртуальных частных сетей
22. Классификация вредоносного программного обеспечения. Антивирусные программы
23. Сетевые модели передачи данных. Модель взаимодействия открытых систем OSI/ISO. Стек протоколов TCP/IP
24. Классификация удаленных угроз в вычислительных сетях
25. Предмет и задачи криптографии и криптоанализа. Стойкость криптографического алгоритма. Классификация криптографических алгоритмов

26. Классические шифры перестановки: шифр «скитала», решетка Кардано и шифр Ришелье. Шифры простой замены: квадрат Полибия, шифрующая система Цезаря. Криптоанализ шифров простой замены
27. Таблица Тритемия, шифровальный диск Альберти.
28. Шифр Вижинера. Шифр Вернама. Шифры колонной замены. Шифровальные машины
29. Основы теории Шенонна и ее развитие. Модели шифров. Результаты теории информации для криптографии
30. Композиции шифров. Сеть Фейстеля
31. Алгоритм шифрования DES, основные режимы работы
32. Шифр AES
33. Вычислительная стойкость криптоалгоритмов. Атаки на алгоритмы шифрования
34. Методы криптоанализа блочных шифров. Требования, предъявляемые к современным блочным алгоритмам шифрования
35. Генерация, распределение и хранение ключей шифрования для симметричных систем, генераторы случайных и псевдослучайных чисел
36. Ассиметричные системы шифрования, их особенности, преимущества и недостатки. Сравнение с симметричными системами
37. Система Диффи-Хеллмана
38. Математические основы асимметричной криптографии.
39. Шифр Шамира. Шифр Эль-Гамаля
40. Шифр RSA. Атаки на алгоритм RSA
41. Гибридные криптосистемы
42. Целостность данных. Функции хэширования. Требования к хэш-функциям
43. Общие положения электронной цифровой подписи. Алгоритмы цифровой подписи RSA и DSA
44. Схема подписи Эль-Гамаля
45. Системы тайного электронного голосования. Электронные деньги. Электронная жеребьевка. Защита документов и ценных бумаг от подделки. Стеганографические методы защиты информации. Системы встраивания информации в изображения, видео и звуковые сигналы
46. Угрозы сообщению. Угрозы пользователю. Угрозы системе
47. Протоколы шифрования/дешифрования в стандартах подвижной связи GSM и CDMA

48. Алгоритмы шифрования, идентификации и аутентификации в стандарте LTE
49. Аутентификация, основанная на алгоритмах симметричного и асимметричного шифрования Обеспечение целостности и конфиденциальности передаваемых данных. Взаимная аутентификация ридера и транспондера
50. Проблемы и особенности организации защиты смарт-карт

4.2. Образец варианта теста итогового контроля

Билет № 5

ФИО студента

1. Перестановочным шифром является:
- **a.** шифр Цезаря;
- **b.** шифр Вижинера;
- **c.** «решетка Кардано»

2. **Шифром сложной замены является:**
- **a.** шифр Цезаря;
- **b.** шифр Вижинера;
- **c.** двойная перестановка

3. **Шифром простой замены является:**
- **a.** шифр гаммирования
- **b.** шифр колонной замены
- **c.** «квадрат Полибия».

4. **Шифры сложной замены являются:**
- **a.** одноалфавитными;
- **b.** многоалфавитными;
- **c.** композиционными.

5. Блочными являются классические шифры:
- **a.** простой замены;
- **b.** сложной замены;
- **c.** перестановки.

6. Режим работы шифров ... производит шифрование и расшифрование блоков текста независимо друг от друга:
- **a.** электронная кодовая книга **ECB;**
- **b.** сцепление блоков шифротекста **CBC**;
- **c.** обратная связь по шифротексту **CFB.**

7. Изменение в среднем половины бит выходного блока алгоритма шифрования при изменении одного бита входного текста называется … шифра:
- **a.** лавинным эффектом;
- **b.** компроментацией;
- **c.** гаммированием**.**

8. **Предметом криптоанализа являются методы:**

- **a.** имитозашиты сообщений;
- **b.** шифрования данных;
- **c.** вскрытия шифров.

9. Длина ключа современного симметричного шифра должна составлять не менее … бит для обеспечения практической стойкости:

- **a.** 64;
- **b.** 128;
- **c.** 256**.**

10. 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.