МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Директор департамента образования

Документ подписан электронной подписью
Сертификат: 1c6cfa0a-52a6-4f49-aef0-5584d3fd4820
Владелец: Троян Павел Ефимович
Действителен: с 19.01.2016 по 16.09.2019

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки / специальность: **09.03.02 Информационные системы и технологии**
Направленность (профиль) / специализация: **Аналитические информационные системы**
Форма обучения: **очная**
Факультет: **ФВС, Факультет вычислительных систем**
Кафедра: **ЭМИС, Кафедра экономической математики, информатики и статистики**
Курс: **4**
Семестр: **7**
Учебный план набора 2015 года

Распределение рабочего времени

№	Виды учебной деятельности	7 семестр	Всего	Единицы
1	Лекции	18	18	часов
2	Лабораторные работы	36	36	часов
3	Всего аудиторных занятий	54	54	часов
4	Самостоятельная работа	126	126	часов
5	Всего (без экзамена)	180	180	часов
6	Подготовка и сдача экзамена	36	36	часов
7	Общая трудоемкость	216	216	часов
		6.0	6.0	З.Е.

Экзамен: 7 семестр

Томск 2018

Рассмотрена и одобрена на заседании кафедры
протокол № 10 от «23» 4 2018 г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 09.03.02 Информационные системы и технологии, утвержденного 12.03.2015 года, рассмотрена и одобрена на заседании кафедры ЭМИС «___» _____ 20__ года, протокол №_____.

Разработчик:
доцент каф. ЭМИС _____ Е. А. Шельмина

Заведующий обеспечивающей каф. ЭМИС _____ И. Г. Боровской

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан ФВС _____ Л. А. Козлова

Заведующий выпускающей каф. ЭМИС _____ И. Г. Боровской

Эксперты:

Профессор кафедры экономической математики, информатики и статистики (ЭМИС) _____ И. Г. Боровской

Профессор кафедры экономической математики, информатики и статистики (ЭМИС) _____ С. И. Колесникова

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Дать представление о сущности и значении информации в развитии современного информационного общества, о необходимости соблюдения основных требований к информационной безопасности. Научить использовать современные компьютерные технологии поиска информации для решения профессиональных задач.

1.2. Задачи дисциплины

– дать будущим специалистам необходимые для их работы теоретические знания о современных средствах, методах и технологиях обеспечения информационной безопасности;

– сформировать у студентов практические навыки организации работ по обеспечению информационной безопасности на предприятиях.

2. Место дисциплины в структуре ОПОП

Дисциплина «Информационная безопасность» (Б1.В.ОД.5) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Дискретная математика, Интеллектуальные системы и технологии, Практика по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности.

Последующими дисциплинами являются: Инструментальные средства информационных систем.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ОПК-4 пониманием сущности и значения информации в развитии современного информационного общества, соблюдение основных требований к информационной безопасности, в том числе защите государственной тайны;

– ОПК-5 способностью использовать современные компьютерные технологии поиска информации для решения поставленной задачи, критического анализа этой информации и обоснования принятых идей и подходов к решению;

– ПК-25 способностью использовать математические методы обработки, анализа и синтеза результатов профессиональных исследований;

В результате изучения дисциплины обучающийся должен:

– **знать** значение информации в развитии современного информационного общества; основные требования к информационной безопасности, в том числе защите государственной тайны; современные компьютерные технологии поиска информации для решения поставленной задачи; математические методы обработки, анализа и синтеза результатов профессиональных исследований;

– **уметь** применять основные требования к информационной безопасности при решении профессиональных задач; использовать современные компьютерные технологии поиска информации для решения поставленной задачи, критического анализа этой информации и обоснования принятых идей и подходов к решению; использовать математические методы обработки, анализа и синтеза результатов профессиональных исследований;

– **владеть** навыками применения основных требований к информационной безопасности при решении профессиональных задач; навыками использования современных компьютерных технологий поиска информации для решения поставленной задачи; навыками применения математических методов при обработке, анализе и синтезе результатов профессиональных исследований;

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 6.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры

		7 семестр
Аудиторные занятия (всего)	54	54
Лекции	18	18
Лабораторные работы	36	36
Самостоятельная работа (всего)	126	126
Оформление отчетов по лабораторным работам	60	60
Проработка лекционного материала	66	66
Всего (без экзамена)	180	180
Подготовка и сдача экзамена	36	36
Общая трудоемкость, ч	216	216
Зачетные Единицы	6.0	6.0

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

Названия разделов дисциплины	Лек., ч	Лаб. раб., ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
7 семестр					
1 Введение	1	0	10	11	ОПК-4, ПК-25
2 Проблемы и методы защиты информации	5	0	8	13	ОПК-4, ОПК-5, ПК-25
3 Математические и методологические средства защиты информации	6	0	38	44	ОПК-4, ОПК-5
4 Криптографические алгоритмы обеспечения информационной безопасности.	4	0	26	30	ОПК-4, ОПК-5
5 Компьютерные средства реализации защиты в информационных системах	2	0	10	12	ОПК-4, ПК-25
6 Шифрование и дешифрирование информации. Реализация методов защиты информации. Метод Полибия	0	10	10	20	ОПК-4, ОПК-5, ПК-25
7 Разработка программы шифрования на основе метода замены	0	8	8	16	ОПК-4, ОПК-5, ПК-25
8 Разработка программы шифрования на основе метода умножения матриц	0	8	6	14	ОПК-4, ОПК-5, ПК-25
9 Разработка программной реализации асимметричного алгоритма шифрования данных RSA	0	6	6	12	ОПК-4, ОПК-5, ПК-25
10 Комплекс криптоалгоритмов PGP	0	4	4	8	ОПК-4, ОПК-5, ПК-25
11 Исторические шифры	0	0	0	0	

12 Основные понятия криптографии	0	0	0	0	
13 Компьютерные алгоритмы шифрования	0	0	0	0	
14 Компьютерная безопасность и практическое применение криптографии	0	0	0	0	
Итого за семестр	18	36	126	180	
Итого	18	36	126	180	

5.2. Содержание разделов дисциплины (по лекциям)

Содержание разделов дисциплин (по лекциям) приведено в таблице 5.2.

Таблица 5.2 – Содержание разделов дисциплин (по лекциям)

Названия разделов	Содержание разделов дисциплины по лекциям	Трудоемкость, ч	Формируемые компетенции
7 семестр			
1 Введение	Цель и задачи дисциплины, ее роль и место в общей системе подготовки специалиста. Защита информации и информационная безопасность как важный фактор политической и экономической составляющих национальной безопасности. Программа информационной безопасности России и пути ее реализации.	1	ОПК-4, ПК-25
	Итого	1	
2 Проблемы и методы защиты информации	Информационная безопасность. Проблемы защиты информации в компьютерных системах. Защита информации при реализации информационных процессов ввода, вывода, передачи, обработки, накопления и хранения информации. Организационное обеспечение информационной безопасности.	5	ОПК-4, ОПК-5, ПК-25
	Итого	5	
3 Математические и методологические средства защиты информации	Криптографическая терминология. Сведения из теории информации и теории чисел. Алгоритмы и ключи. Симметричные алгоритмы. Алгоритмы с открытым ключом. Подстановочные и перестановочные шифры. Одноразовые блокноты. Однонаправленные хэш-функции. Передача информации с использованием криптографии с открытым ключом. Основные протоколы передачи информации.	6	ОПК-4
	Итого	6	
4 Криптографические алгоритмы обеспечения информационной безопасности.	Алгоритм симметричного шифрования данных DES. Алгоритм криптографического преобразования ГОСТ 28147-89. Асимметричный алгоритм шифрования данных RSA. Комплекс криптографических алгоритмов PGP. Защита информации от несанкционированного доступа.	4	ОПК-4, ОПК-5

	Итого	4	
5 Компьютерные средства реализации защиты в информационных системах	Физический, сетевой, транспортный и прикладной уровни защиты информации. Обзор стандартов в области защиты информации. Методы и средства защиты локальной рабочей станции. Защита в локальных сетях. Защита информации при межсетевом взаимодействии. Типы вирусов и средства антивирусной защиты. Обеспечение информационной безопасности в корпоративных сетях.	2	ОПК-4, ПК-25
	Итого	2	
Итого за семестр		18	

5.3. Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами

Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами представлены в таблице 5.3.

Таблица 5.3 – Разделы дисциплины и междисциплинарные связи

Наименование дисциплин	№ разделов данной дисциплины, для которых необходимо изучение обеспечивающих и обеспечиваемых дисциплин													
	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Предшествующие дисциплины														
1 Дискретная математика			+											
2 Интеллектуальные системы и технологии												+		
3 Практика по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности		+	+	+								+		
Последующие дисциплины														
1 Инструментальные средства информационных систем		+		+										

5.4. Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий представлено в таблице 5.4.

Таблица 5.4 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

	Виды занятий	Формы контроля

Компетенции	Лек.	Лаб. раб.	Сам. раб.	
ОПК-4	+	+	+	Экзамен, Коллоквиум, Отчет по лабораторной работе, Тест
ОПК-5	+	+	+	Экзамен, Коллоквиум, Отчет по лабораторной работе, Тест
ПК-25	+	+	+	Экзамен, Коллоквиум, Отчет по лабораторной работе, Тест

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП.

7. Лабораторные работы

Наименование лабораторных работ приведено в таблице 7.1.

Таблица 7.1 – Наименование лабораторных работ

Названия разделов	Наименование лабораторных работ	Трудоемкость, ч	Формируемые компетенции
7 семестр			
6 Шифрование и дешифрирование информации. Реализация методов защиты информации. Метод Полибия	Шифрование и дешифрование методом Полибия.	10	ОПК-4, ОПК-5, ПК-25
	Итого	10	
7 Разработка программы шифрования на основе метода замены	Шифрование и дешифрование с помощью метода замены	8	ОПК-4, ОПК-5, ПК-25
	Итого	8	
8 Разработка программы шифрования на основе метода умножения матриц	Шифрование сообщения методом произведения матриц.	8	ОПК-4, ОПК-5, ПК-25
	Итого	8	
9 Разработка программной реализации асимметричного алгоритма шифрования данных RSA	Разработка программной реализации алгоритма RSA.	6	ОПК-4, ОПК-5, ПК-25
	Итого	6	
10 Комплекс криптоалгоритмов PGP	Использование комплекса PGP	4	ОПК-4, ОПК-5, ПК-25
	Итого	4	
Итого за семестр		36	

8. Практические занятия (семинары)

Не предусмотрено РУП.

9. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 9.1.

Таблица 9.1 – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
7 семестр				
1 Введение	Проработка лекционного материала	10	ОПК-4	Коллоквиум
	Итого	10		
2 Проблемы и методы защиты информации	Проработка лекционного материала	8	ОПК-4, ОПК-5	Коллоквиум, Тест
	Итого	8		
3 Математические и методологические средства защиты информации	Проработка лекционного материала	22	ОПК-4, ОПК-5	Коллоквиум, Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	16		
	Итого	38		
4 Криптографические алгоритмы обеспечения информационной безопасности.	Проработка лекционного материала	16	ОПК-4, ОПК-5	Коллоквиум, Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	10		
	Итого	26		
5 Компьютерные средства реализации защиты в информационных системах	Проработка лекционного материала	10	ОПК-4	Коллоквиум
	Итого	10		
6 Шифрование и дешифрирование информации. Реализация методов защиты информации. Метод Полибия	Оформление отчетов по лабораторным работам	10	ОПК-4, ОПК-5, ПК-25	Отчет по лабораторной работе, Тест
	Итого	10		
7 Разработка программы шифрования на основе метода замены	Оформление отчетов по лабораторным работам	8	ОПК-4, ОПК-5, ПК-25	Отчет по лабораторной работе, Тест
	Итого	8		
8 Разработка программы шифрования на основе метода умножения матриц	Оформление отчетов по лабораторным работам	6	ОПК-4, ОПК-5, ПК-25	Отчет по лабораторной работе, Тест
	Итого	6		
9 Разработка программной	Оформление отчетов по лабораторным работам	6	ОПК-4, ОПК-5,	Отчет по лабораторной работе, Тест

реализации асимметричного алгоритма шифрования данных RSA	Итого	6	ПК-25	
10 Комплекс криптоалгоритмов PGP	Оформление отчетов по лабораторным работам	4	ОПК-4, ОПК-5, ПК-25	Отчет по лабораторной работе, Тест
	Итого	4		
Итого за семестр		126		
	Подготовка и сдача экзамена	36		Экзамен
Итого		162		

10. Курсовая работа (проект)

Не предусмотрено РУП.

11. Рейтинговая система для оценки успеваемости обучающихся

11.1. Балльные оценки для элементов контроля

Таблица 11.1 – Балльные оценки для элементов контроля

Элементы учебной деятельности	Максимальный балл на 1-ую КТ с начала семестра	Максимальный балл за период между 1КТ и 2КТ	Максимальный балл за период между 2КТ и на конец семестра	Всего за семестр
7 семестр				
Коллоквиум	5	5	5	15
Отчет по лабораторной работе	15	25	15	55
Итого максимум за период	20	30	20	70
Экзамен				30
Нарастающим итогом	20	50	70	100

11.2. Пересчет баллов в оценки за контрольные точки

Пересчет баллов в оценки за контрольные точки представлен в таблице 11.2.

Таблица 11.2 – Пересчет баллов в оценки за контрольные точки

Баллы на дату контрольной точки	Оценка
≥ 90% от максимальной суммы баллов на дату КТ	5
От 70% до 89% от максимальной суммы баллов на дату КТ	4
От 60% до 69% от максимальной суммы баллов на дату КТ	3
< 60% от максимальной суммы баллов на дату КТ	2

11.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 11.3.

Таблица 11.3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка (ГОС)	Итоговая сумма баллов, учитывает успешно сданный экзамен	Оценка (ECTS)
5 (отлично) (зачтено)	90 - 100	A (отлично)

4 (хорошо) (зачтено)	85 - 89	B (очень хорошо)
	75 - 84	C (хорошо)
	70 - 74	D (удовлетворительно)
3 (удовлетворительно) (зачтено)	65 - 69	
	60 - 64	E (посредственно)
2 (неудовлетворительно) (не зачтено)	Ниже 60 баллов	F (неудовлетворительно)

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс] : учеб. пособие — Электрон. дан. — Москва : Горячая линия-Телеком, 2013. — 338 с. [Электронный ресурс]. - https://e.lanbook.com/book/63235

12.2. Дополнительная литература

1. Бабенко, Л.К. Параллельные алгоритмы для решения задач защиты информации [Электронный ресурс] : учеб. пособие / Л.К. Бабенко, Е.А. Ищукова, И.Д. Сидоров. — Электрон. дан. — Москва : Горячая линия-Телеком, 2014. — 304 с. [Электронный ресурс]. - https://e.lanbook.com/book/63228

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Защита информации: Методические указания к выполнению самостоятельных работ / Спицын В. Г. - 2012. 78 с. [Электронный ресурс] - Режим доступа: http://edu.tusur.ru/publications/2261, дата обращения: 03.05.2018.
2. Защита информации: Методические указания к выполнению лабораторных работ / Спицын В. Г. - 2012. 17 с. [Электронный ресурс] - Режим доступа: http://edu.tusur.ru/publications/1822, дата обращения: 03.05.2018.

12.3.2. Учебно-методические пособия для лиц с ограниченными возможностями здоровья и инвалидов

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа лиц с ограниченными возможностями здоровья и инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

Для лиц с нарушениями зрения:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

12.4. Профессиональные базы данных и информационные справочные системы

1. Информационно-аналитическая система Science Index РИНЦ - https://elibrary.ru/defaultx.asp
2. Информационная система - https://uisrussia.msu.ru

13. Материально-техническое обеспечение дисциплины и требуемое программное обеспечение

13.1. Общие требования к материально-техническому и программному обеспечению дисциплины

13.1.1. Материально-техническое и программное обеспечение для лекционных занятий

Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория с количеством посадочных мест не менее 22-24, оборудованная доской и стандартной учебной мебелью. Имеются демонстрационное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

13.1.2. Материально-техническое и программное обеспечение для лабораторных работ

Лаборатория ГПО / «Лаборатория подготовки разработчиков бизнес-приложений»

учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа, помещение для курсового проектирования (выполнения курсовых работ), помещение для проведения групповых и индивидуальных консультаций, помещение для проведения текущего контроля и промежуточной аттестации, помещение для самостоятельной работы

634034, Томская область, г. Томск, Вершинина улица, д. 74, 425 ауд.

Описание имеющегося оборудования:

- ПЭВМ (Intel Pentium G3220, 3 G, 4 Gb RAM) (12 шт.);
- Плазменный телевизор;
- Магнито-маркерная доска;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- 7-Zip
- Google Chrome
- Microsoft Visual Studio 2012
- OpenOffice

13.1.3. Материально-техническое и программное обеспечение для самостоятельной работы

Для самостоятельной работы используются учебные аудитории (компьютерные классы), расположенные по адресам:

- 634050, Томская область, г. Томск, Ленина проспект, д. 40, 233 ауд.;
- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 201 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Состав оборудования:

- учебная мебель;
- компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 5 шт.;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета.

Перечень программного обеспечения:

- Microsoft Windows;
- OpenOffice;
- Kaspersky Endpoint Security 10 для Windows;
- 7-Zip;
- Google Chrome.

13.2. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья и инвалидов

Освоение дисциплины лицами с ограниченными возможностями здоровья и инвалидами осуществляется с использованием средств обучения общего и специального назначения.

При занятиях с обучающимися **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах, мобильной системы преподавания для обучающихся с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой занимаются обучающиеся с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При занятиях с обучающимися **с нарушениями зрениями** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для комфортного просмотра.

При занятиях с обучающимися **с нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах, мобильной системы обучения для людей с инвалидностью.

14. Оценочные материалы и методические рекомендации по организации изучения дисциплины

14.1. Содержание оценочных материалов и методические рекомендации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы в составе:

14.1.1. Тестовые задания

Количество знаков в шифротексте и в исходном тексте в общем случае:

не может различаться

может различаться

должно быть равно сумме знаков открытого текста и ключа

должно быть равно разности знаков открытого текста и ключа

Стойкость современных криптосистем основывается на:

секретности долговременных элементов криптозащиты

применении стеганографических алгоритмов

секретности алгоритма шифрования

секретности информации сравнительно малого размера, называемой ключом

Идентификация законных пользователей заключается в:

сравнении пароля, вводимого пользователем, с паролем, хранящимся в явном виде в ЭВМ

сравнении пароля, вводимого пользователем, с образом пароля, хранящимся в ЭВМ

сравнении образа пароля, вводимого пользователем, с образом пароля, хранящегося в явном виде в ЭВМ

сравнении пароля, вводимого пользователем, с открытым ключом, хранящимся в ЭВМ

Протокол — это:

совокупность действий, выполняемых в случайной последовательности двумя или более субъектами с целью достижения определенного результата

совокупность действий, выполняемых в заданной последовательности двумя или более субъектами с целью достижения определенного результата

совокупность действий, выполняемых в заданной последовательности одним субъектом с целью достижения определенного результата

совокупность действий, выполняемых в случайной последовательности одним субъектом с целью достижения определенного результата

Подстановочным шифром называется шифр, в котором:

используется матрица чисел размерностью 5x5

используется открытый ключ

используется фрагмент текста и открытый ключ

каждый символ открытого текста в шифротексте заменяется другим символом

В шифровании с использованием одноразовых блокнотов должны выполняться условия:
ключ должен быть псевдослучайным и может применяться только один раз
ключ должен быть случайным, может применяться только один раз и длина ключа равна длине сообщения
ключ должен быть случайным, может применяться постоянно и длина ключа произвольна
ключ должен быть псевдослучайным, может применяться только один раз и длина ключа равна длине сообщения
В шифре Цезаря каждый символ открытого текста:
заменяется символом, находящимся двумя символами правее по модулю 26
заменяется символом, находящимся семью символами правее по модулю 26
заменяется символом, находящимся тремя символами правее по модулю 26
заменяется символом, находящимся пятью символами правее по модулю 26
В операции “исключающее или” (XOR):
0+0=1; 0+1=1; 1+0=1; 1+1=0
0+0=0; 0+1=0; 1+0=1; 1+1=0
0+0=1; 0+1=1; 1+0=0; 1+1=0
0+0=0; 0+1=1; 1+0=1; 1+1=0
Для случайного набора символов индекс совпадений равен:
0.871
0.038
0.001
0.135
Для осмысленного текста, написанного на английском языке индекс совпадений равен:
0.521
0.332
0.024
0.065
Безопасность симметричного алгоритма определяется:
применением разных ключей для шифрования и дешифрования
ключом
применением двух ключей
литературными данными
Асимметричный шифр отличается от симметричного тем, что:
ключ шифрования отличается от ключа дешифрования
ключ дешифрирования может быть рассчитан по ключу шифрования
ключ шифрования совпадает с ключом дешифрования
используются несколько ключей для шифрования
Алгоритмы с открытыми ключами не заменяют симметричные алгоритмы и используются не для шифрования сообщений, а для шифрования ключей, потому что:
работают медленнее в 2 раза
являются такими же стойкими к вскрытию при работе с выбранным открытым текстом, но более сложными
работают медленнее в 1000 раз
применяются три ключа
Смешанные криптосистемы основаны на совместном применении:
симметричных алгоритмов и алгоритмов с открытыми ключами
нескольких двухключевых алгоритмов
нескольких одноключевых алгоритмов
потоковых и блочных алгоритмов
Сеансовый ключ в смешанных криптосистемах – это:
открытый ключ смешанной криптосиситемы
закрытый ключ алгоритма с открытым ключом
ключ симметричного алгоритма смешанной криптосиситемы, использующийся один раз
ключ, смоделированный из двух ключей алгоритма с открытым ключом

Для данного языка абсолютная норма языка равна R=log2L, где L:

количество возможных значений сообщения

длина сообщения

размер пространства ключей

число символов в алфавите

Приведенным множеством остатков mod n, называется подмножество множества остатков, члены которого взаимно просты с n (НОД(a,n)=1). Например, для mod 14, это:

{1,3,4,5,6,8,9,11,13}

{1,3,5,9,11,13}

{1,5,9,11,13}

{1,3,5,9,11}

В симметричном поточном шифре, использующем операцию исключающего ИЛИ, биты шифротекста получаются по правилу: Ci=mi+ki, где m0,m1, . . . – биты открытого текста, а k0, k1, . . . – биты ключевого потока. Открытый текст – 1100101010, поток ключей – 1010011001, тогда шифротекст это:

1010101111

0111001110

0110110011

0101010001

Основными характеристиками итерированных блочных шифров являются: размер блока в битах, длина ключа в битах, число раундов шифрования. Для шифра DES это:

64, 56, 16

64, 128, 16

64, 64, 32

128, 56, 32

В шифре DES применяется количество подключей n, причем каждый из подключей имеет размер m бит:

n=64, m=256

n=32, m=64

n=8, m=32

n=16, m=48

14.1.2. Экзаменационные вопросы

Защита информации и информационная безопасность как важный фактор политической и экономической составляющих национальной безопасности.

Программа информационной безопасности России и пути ее реализации.

Проблемы защиты информации в компьютерных системах.

Защита информации при реализации информационных процессов ввода, вывода, передачи, обработки, накопления и хранения информации.

Организационное обеспечение информационной безопасности.

Криптографическая терминология.

Алгоритмы и ключи.

Симметричные алгоритмы.

Алгоритмы с открытым ключом.

Подстановочные и перестановочные шифры.

Одноразовые блокноты.

Однонаправленные хэш-функции.

Передача информации с использованием криптографии с открытым ключом.

Алгоритм симметричного шифрования данных DES.

Асимметричный алгоритм шифрования данных RSA.

Комплекс криптографических алгоритмов PGP.

Защита информации от несанкционированного доступа.

Физический, сетевой, транспортный и прикладной уровни защиты информации.

Обзор стандартов в области защиты информации.

Методы и средства защиты локальной рабочей станции.

Защита в локальных сетях.
Защита информации при межсетевом взаимодействии.
Типы вирусов и средства антивирусной защиты.
Обеспечение информационной безопасности в корпоративных сетях.

14.1.3. Темы коллоквиумов

Сформулируйте правило Керкхоффа относительно стойкости шифра.
Опишите принцип реализации электронной цифровой подписи.
Охарактеризуйте моноалфавитный, однозвучный, и полиграмный подстановочные шифры.
Охарактеризуйте операцию XOR.
Опишите столбцовый перестановочный шифр.
Дайте определение криптографического протокола.
Опишите схему вскрытия сообщения, зашифрованного моноалфавитным шифром замены.
Каким образом можно определить понятие однонаправленной хэш-функции?
Охарактеризуйте смешанные криптосистемы.
Каким образом осуществляется передача ключей и сообщений без предварительного выполнения протокола обмена ключами?
Опишите способ подписи документа на основе криптографии с открытыми ключами.
Опишите свойства меток времени в электронных цифровых подписях документов?
Каким образом норма языка выражается через энтропию и длину сообщения?
Определите понятие абсолютной нормы языка.
Определите понятие расстояния уникальности.
Опишите упрощенную модель шифрования битовой строки.
Приведите схему и опишите принцип работы поточного шифра.
Приведите схему и опишите принцип работы блочного шифра.
Охарактеризуйте основные операции и приведите блок-схему работы шифра Фейстеля.
Охарактеризуйте основные операции и приведите блок-схему работы шифра DES.
Приведите описание алгоритма с открытым ключом RSA.
Какие технологии шифрования применяются в PGP?

14.1.4. Темы лабораторных работ

Шифрование и дешифрование методом Полибия.
Шифрование и дешифрование с помощью метода замены
Шифрование сообщения методом произведения матриц.
Разработка программной реализации алгоритма RSA.
Использование комплекса PGP

14.2. Требования к оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусмотрены дополнительные оценочные материалы, перечень которых указан в таблице 14.

Таблица 14 – Дополнительные материалы оценивания для лиц с ограниченными возможностями здоровья и инвалидов

Категории обучающихся	Виды дополнительных оценочных материалов	Формы контроля и оценки результатов обучения
С нарушениями слуха	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы	Преимущественно письменная проверка
С нарушениями зрения	Собеседование по вопросам к зачету, опрос по терминам	Преимущественно устная проверка (индивидуально)
С нарушениями опорно-двигательного аппарата	Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету	Преимущественно дистанционными методами

С ограничениями по общемедицинским показаниям	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы	Преимущественно проверка методами исходя из состояния обучающегося на момент проверки

14.3. Методические рекомендации по оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной форме;
- в печатной форме с увеличенным шрифтом;
- в форме электронного документа;
- методом чтения ассистентом задания вслух;
- предоставление задания с использованием сурдоперевода.

Лицам с ограниченными возможностями здоровья и инвалидам увеличивается время на подготовку ответов на контрольные вопросы. Для таких обучающихся предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге;
- набор ответов на компьютере;
- набор ответов с использованием услуг ассистента;
- представление ответов устно.

Процедура оценивания результатов обучения лиц с ограниченными возможностями здоровья и инвалидов по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

При необходимости для лиц с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения может проводиться в несколько этапов.