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
_____ П. Е. Троян
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки / специальность: **09.03.03 Прикладная информатика**
Направленность (профиль) / специализация: **Прикладная информатика в области экономики**
Форма обучения: **заочная**
Факультет: **ЗиВФ, Заочный и вечерний факультет**
Кафедра: **АСУ, Кафедра автоматизированных систем управления**
Курс: **4**
Семестр: **7, 8**
Учебный план набора 2014 года

Распределение рабочего времени

№	Виды учебной деятельности	7 семестр	8 семестр	Всего	Единицы
1	Лекции	4	4	8	часов
2	Практические занятия	4	0	4	часов
3	Лабораторные работы	0	6	6	часов
4	Всего аудиторных занятий	8	10	18	часов
5	Самостоятельная работа	64	89	153	часов
6	Всего (без экзамена)	72	99	171	часов
7	Подготовка и сдача экзамена	0	9	9	часов
8	Общая трудоемкость	72	108	180	часов
				5.0	З.Е.

Контрольные работы: 7 семестр - 1
Экзамен: 8 семестр

Томск 2018

Согласована на портале № 32050

Рассмотрена и одобрена на заседании кафедры
протокол № 6 от «17» 5 2018 г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 09.03.03 Прикладная информатика, утвержденного 27.03.2015 года, рассмотрена и одобрена на заседании кафедры АСУ «___» _____ 20__ года, протокол №_____.

Разработчик:

профессор каф. АСУ	_____	А. Н. Горитов
Заведующий обеспечивающей каф. АСУ	_____	А. М. Кориков

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан ЗиВФ	_____	И. В. Осипов
Заведующий выпускающей каф. АСУ	_____	А. М. Кориков

Эксперты:

Заведующий кафедрой автоматизированных систем управления (АСУ)	_____	А. М. Кориков
Доцент кафедры автоматизированных систем управления (АСУ)	_____	А. И. Исакова

Согласована на портале № 32050

1. Цели и задачи дисциплины

1.1. Цели дисциплины

дать студентам необходимые знания, умения и навыки в области современных информационных технологий, применяемых в настоящее время, а также защиты информации.

1.2. Задачи дисциплины

– овладение теоретическими знаниями в области информационных технологий и обеспечения их безопасности, а также управления информационными ресурсами;

– приобретение прикладных знаний в области создания систем защиты информации, а также оптимизации моделей сложных процессов бизнеса;

– овладение навыками самостоятельного использования соответствующих инструментальных программных систем.

2. Место дисциплины в структуре ОПОП

Дисциплина «Информационная безопасность» (Б1.Б.19) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Информационная безопасность, Дискретная математика, Информатика и программирование, Математика, Операционные системы, Основы алгоритмизации и языки программирования, Программная инженерия, Проектирование информационных систем.

Последующими дисциплинами являются: Информационная безопасность, Проектный практикум, Сетевая экономика.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ОПК-4 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

В результате изучения дисциплины обучающийся должен:

– **знать** основные понятия и принципы защиты информации; современные подходы к защите продуктов и систем информационных технологий; основные методы обеспечения многоуровневой безопасности в информационных системах.

– **уметь** выявлять угрозы информационной безопасности; использовать средства защиты данных для организации безопасной работы компьютеров.

– **владеть** навыками применения методов и средств защиты информации для обеспечения информационной безопасности на предприятии или организации.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 5.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры	
		7 семестр	8 семестр
Аудиторные занятия (всего)	18	8	10
Лекции	8	4	4
Практические занятия	4	4	
Лабораторные работы	6		6
Самостоятельная работа (всего)	153	64	89
Оформление отчетов по лабораторным работам	19	0	19
Проработка лекционного материала	110	40	70

Согласована на портале № 32050

Самостоятельное изучение тем (вопросов) теоретической части курса	10	10	0
Подготовка к практическим занятиям, семинарам	8	8	0
Выполнение контрольных работ	6	6	0
Всего (без экзамена)	171	72	99
Подготовка и сдача экзамена	9	0	9
Общая трудоемкость, ч	180	72	108
Зачетные Единицы	5.0		

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	Прак. зан., ч	Лаб. раб., ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
7 семестр						
1 Введение в информационную безопасность.	1	2	0	4	7	ОПК-4
2 Математические методы и модели в задачах защиты информации.	1	2	0	34	37	ОПК-4
3 Математические основы криптографических методов.	1	0	0	14	15	ОПК-4
4 Криптография с открытым ключом.	1	0	0	12	13	ОПК-4
Итого за семестр	4	4	0	64	72	
8 семестр						
5 Методы идентификации и аутентификации пользователей.	1	0	0	29	30	ОПК-4
6 Межсетевые экраны и VPN сети.	1	0	4	18	23	ОПК-4
7 Защита компьютерных систем от вредоносных программ.	1	0	0	16	17	ОПК-4
8 Комплексная защита информации.	1	0	2	26	29	ОПК-4
Итого за семестр	4	0	6	89	99	
Итого	8	4	6	153	171	

Согласована на портале № 32050

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 в информационную безопасность.	Исторические аспекты и современная постановка задач обеспечения информационной безопасности и защиты информации. Основные понятия и определения: конфиденциальность, целостность, доступность, угроза, уязвимость, риски. Основы российского законодательства в сфере защиты информации.	1	ОПК-4
	Итого	1	
2 Математические методы и модели в задачах защиты информации.	Основные понятия и определения криптографии. Краткая история развития криптологии. Классификация методов шифрования. Блочные шифры. Алгоритмы блочного шифрования. Вопросы стойкости блочных шифров. Потоковые шифры. Основные понятия. Алгоритмы потокового шифрования.	1	ОПК-4
	Итого	1	
3 Математические основы криптографических методов.	Основные понятия и определения теории информации. Основные теоремы теории чисел. Дискретные логарифмы в конечном поле. Элементы теории сложности проблем.	1	ОПК-4
	Итого	1	
4 Криптография с открытым ключом.	Криптография с открытым ключом. Основные способы использования алгоритмов с открытым ключом. Задача распределения ключей. Алгоритмы шифрования с открытым ключом. Криптографические хеш-функции. Электронная цифровая подпись. Основные процедуры цифровой подписи. Алгоритмы электронной цифровой подписи. Сертификат открытого ключа.	1	ОПК-4
	Итого	1	
Итого за семестр		4	
8 семестр			
5 Методы идентификации и аутентификации пользователей.	Основные понятия и определения. Понятие криптографического протокола. Методы аутентификации на основе паролей. Методы строгой аутентификации. Биометрическая аутентификация пользователя.	1	ОПК-4
	Итого	1	
6 Межсетевые экраны и VPN сети.	Межсетевые экраны. Режимы функционирования межсетевых экранов и их основные компоненты.	1	ОПК-4

Согласована на портале № 32050

	Основные схемы сетевой защиты на базе межсетевых экранов. Виртуальные защищенные сети. Основы построения виртуальных защищенных сетей.		
	Итого	1	
7 Защита компьютерных систем от вредоносных программ.	Вредоносные программы и их классификация. Методы обнаружения и удаления вирусов. Программные закладки и методы защиты от них.	1	ОПК-4
	Итого	1	
8 Комплексная защита информации.	Концепция комплексной защиты информации. Методология создания, организации и обеспечения функционирования систем комплексной защиты информации (КЗИ).	1	ОПК-4
	Итого	1	
Итого за семестр		4	
Итого		8	

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
Предшествующие дисциплины								
1 Информационная безопасность	+	+	+	+	+	+	+	+
2 Дискретная математика	+	+	+	+	+			
3 Информатика и программирование				+	+	+	+	+
4 Математика	+	+	+	+	+	+	+	+
5 Операционные системы				+	+	+	+	+
6 Основы алгоритмизации и языки программирования		+	+	+	+	+	+	+
7 Программная инженерия			+	+	+	+	+	+
8 Проектирование информационных систем	+	+	+	+	+	+	+	+
Последующие дисциплины								
1 Информационная безопасность	+	+	+	+	+	+	+	+
2 Проектный практикум		+	+	+	+	+	+	+
3 Сетевая экономика			+	+	+	+	+	+

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

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Согласована на портале № 32050

представлено в таблице 5.4.

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

Компетенции	Виды занятий				Формы контроля
	Лек.	Прак. зан.	Лаб. раб.	Сам. раб.	
ОПК-4	+	+	+	+	Экзамен, Конспект самоподготовки, Проверка контрольных работ, Отчет по лабораторной работе, Опрос на занятиях, 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
8 семестр			
6 Межсетевые экраны и VPN сети.	Защита информации при обработке и передачи по сетям ЭВМ.	4	ОПК-4
	Итого	4	
8 Комплексная защита информации.	Практическое применение методов защиты информации.	2	ОПК-4
	Итого	2	
Итого за семестр		6	
Итого		6	

8. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 8.1.

Таблица 8.1 – Наименование практических занятий (семинаров)

Названия разделов	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
7 семестр			
1 Введение в информационную безопасность.	Базовые понятия информационной безопасности	2	ОПК-4
	Итого	2	
2 Математические методы и модели в	Методы защиты информации	2	ОПК-4
	Итого	2	

Согласована на портале № 32050

задачах защиты информации.			
Итого за семестр		4	
Итого		4	

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 в информационную безопасность.	Проработка лекционного материала	4	ОПК-4	Опрос на занятиях
	Итого	4		
2 Математические методы и модели в задачах защиты информации.	Выполнение контрольных работ	6	ОПК-4	Конспект самоподготовки, Опрос на занятиях, Проверка контрольных работ, Тест, Экзамен
	Подготовка к практическим занятиям, семинарам	6		
	Самостоятельное изучение тем (вопросов) теоретической части курса	10		
	Проработка лекционного материала	12		
	Итого	34		
3 Математические основы криптографических методов.	Подготовка к практическим занятиям, семинарам	2	ОПК-4	Опрос на занятиях, Тест, Экзамен
	Проработка лекционного материала	12		
	Итого	14		
4 Криптография с открытым ключом.	Проработка лекционного материала	12	ОПК-4	Опрос на занятиях, Тест, Экзамен
	Итого	12		
Итого за семестр		64		
8 семестр				
5 Методы идентификации и аутентификации пользователей.	Проработка лекционного материала	18	ОПК-4	Опрос на занятиях, Отчет по лабораторной работе, Тест, Экзамен
	Оформление отчетов по лабораторным работам	11		
	Итого	29		

Согласована на портале № 32050

6 Межсетевые экраны и VPN сети.	Проработка лекционного материала	18	ОПК-4	Опрос на занятиях, Тест, Экзамен
	Итого	18		
7 Защита компьютерных систем от вредоносных программ.	Проработка лекционного материала	16	ОПК-4	Опрос на занятиях, Тест, Экзамен
	Итого	16		
8 Комплексная защита информации.	Проработка лекционного материала	18	ОПК-4	Опрос на занятиях, Отчет по лабораторной работе, Тест, Экзамен
	Оформление отчетов по лабораторным работам	8		
	Итого	26		
Итого за семестр		89		
	Подготовка и сдача экзамена	9		Экзамен
Итого		162		

10. Курсовой проект / курсовая работа

Не предусмотрено РУП.

11. Рейтинговая система для оценки успеваемости обучающихся

Рейтинговая система не используется.

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах: Учебное пособие для вузов. – М.: ФОРУМ, 2012. – 592 с. (наличие в библиотеке ТУСУР - 30 экз.)

12.2. Дополнительная литература

1. Бацула А.П. Информационная безопасность: Учебное пособие. – Томск: ТУСУР, 2007. – 137 с. (наличие в библиотеке ТУСУР - 25 экз.)

2. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах: Учебн. пособие для вузов. 3-е изд. – М.: Горячая линия – Телеком, 2005. – 144 с. (наличие в библиотеке ТУСУР - 50 экз.)

3. Мельников В.П. Информационная безопасность и защита информации: учебн. пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; ред. : С. А. Клейменов. - М.: Academia, 2006. - 330 с. (наличие в библиотеке ТУСУР - 30 экз.)

4. Куприянов А.И. Основы защиты информации: учебн. пособие для вузов / А. И. Куприянов, А. В. Сахаров, В. А. Шевцов. - М.: Academia, 2006. - 253 с. (наличие в библиотеке ТУСУР - 50 экз.)

5. Основы информационной безопасности: учебн. пособие для вузов / Е.Б. Белов [и др]. – М.: Горячая линия – Телеком, 2006. – 544 с. (наличие в библиотеке ТУСУР - 80 экз.)

6. Партыка Т.Л. Информационная безопасность: Учебное пособие. 3-е изд., исп. и доп. - М.: Форум, 2007. – 367 с. (наличие в библиотеке ТУСУР - 20 экз.)

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Горитов А.Н. Информационная безопасность: методические указания к практическим занятиям. – Томск: ТУСУР, 2011. – 8 с. [Электронный ресурс] - Режим доступа: http://asu.tusur.ru/learning/090303/d40/090303-d40-pract.pdf (дата обращения: 26.06.2018).

2. Горитов А.Н. Информационная безопасность: методические указания по выполнению лабораторных работ. – Томск: ТУСУР, 2011. – 6 с. [Электронный ресурс] - Режим доступа: http://asu.tusur.ru/learning/090303/d40/090303-d40-lab.pdf (дата обращения: 26.06.2018).

Согласована на портале № 32050

3. Горитов А.Н. Информационная безопасность: методические указания по самостоятельной и индивидуальной работе студентов. – Томск: ТУСУР, 2011. – 8 с. [Электронный ресурс] - Режим доступа: http://asu.tusur.ru/learning/090303/d40/090303-d40-work.pdf (дата обращения: 26.06.2018).

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. http://www.edu.tusur.ru – образовательный портал университета;
2. http://www.lib.tusur.ru – веб-сайт библиотеки университета;
3. http://www.elibrary.ru – научная электронная библиотека;
4. http://www.edu.ru – веб-сайт системы федеральных образовательных порталов.

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 практических занятий

Учебная вычислительная лаборатория / Лаборатория ГПО "Мониторинг"

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, 438 ауд.

Описание имеющегося оборудования:

- Рабочие станции: системный блок MB Asus P5B / CPU Intel Core 2 Duo 6400 2.13 GHz / 5Гб RAM DDR2 / 250Gb HDD / LAN (10 шт.);
- Монитор 19 Samsung 931BF (10 шт.);
- Проектор ACER X125H DLP;
- Экран проектора;
- Видеокамера (2 шт.);
- Точка доступа WiFi;
- Комплект специализированной учебной мебели;

Согласована на портале № 32050

- Рабочее место преподавателя.

Программное обеспечение:

- Adobe Acrobat Reader
- Adobe Flash Player
- Code::Blocks
- Far Manager
- Free Pascal
- Lazarus
- LibreOffice
- Microsoft Office 2003
- Microsoft PowerPoint Viewer
- Microsoft Visual Studio 2013 Professional
- Microsoft Windows 7 Pro

13.1.3. Материально-техническое и программное обеспечение для лабораторных работ

Учебная вычислительная лаборатория / Лаборатория ГПО "Мониторинг"

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, 438 ауд.

Описание имеющегося оборудования:

- Рабочие станции: системный блок MB Asus P5B / CPU Intel Core 2 Duo 6400 2.13 GHz / 5Гб RAM DDR2 / 250Gb HDD / LAN (10 шт.);
- Монитор 19 Samsung 931BF (10 шт.);
- Проектор ACER X125H DLP;
- Экран проектора;
- Видеокамера (2 шт.);
- Точка доступа WiFi;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- Adobe Acrobat Reader
- Adobe Flash Player
- Code::Blocks
- Far Manager
- Free Pascal
- Lazarus
- LibreOffice
- Microsoft Office 2003
- Microsoft PowerPoint Viewer
- Microsoft Windows 7 Pro

13.1.4. 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.

Согласована на портале № 32050

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

1. Длина ключа в алгоритме ГОСТ 28147:
25 бит
128 бит
448 бит
256 бит
2. Для передачи коротких сообщений лучше всего соответствуют режимы:
CBC
CFB
OFB
ECB
3. Для передачи больших сообщений лучше всего соответствуют режимы:
ECB
CFB
OFB
CBC
4. Режим CBC используется для того, чтобы
увеличить скорость шифрования

Согласована на портале № 32050

не было необходимости разбивать сообщение на целое число блоков достаточно большой длины

одинаковые незашифрованные блоки преобразовывались в различные зашифрованные блоки

5. Какие виды алгоритмов подразделяются на блочные и поточные
комбинированные
асимметричные
симметричные
6. Длина хеш-кода хеш-функции ГОСТ 3411 равна
128 бит
160 бит
256 бит
7. Длина хеш-кода, создаваемого хеш-функцией MD5, равна
256 бит
160 бит
128 бит
8. Длина хеш-кода, создаваемого хеш-функцией SHA-1, равна
128 бит
256 бит
160 бит
9. Для шифрования сообщения следует использовать
свой открытый ключ
свой закрытый ключ
открытый ключ получателя
10. Хеш-функции предназначены для
сжатия сообщения
шифрования сообщения
получения дайджеста сообщения
11. Алгоритм Диффи-Хеллмана основан на
задаче факторизации числа
задаче определения, является ли данное число простым
задаче дискретного логарифмирования
12. Алгоритм RSA основан на:
задаче дискретного логарифмирования
задаче определения, является ли данное число простым
задаче факторизации числа
13. Для создания подписи следует использовать
закрытый ключ получателя
свой открытый ключ
свой закрытый ключ
14. В DSS используется следующая хеш-функция
MD5
SHA-2
SHA-1
15. В стандарте ГОСТ 3410 используется следующая хеш-функция
MD5
SHA-1
ГОСТ 3411
16. Цифровая подпись вычисляется:
для отправляемого электронного сообщения
для отправляемого сообщения совместно с дайджестом
для отправляемого сообщения и адресом отправителя
для дайджеста отправляемого электронного сообщения
17. Задачей дискретного логарифмирования является...

Согласована на портале № 32050

разложение числа на простые сомножители

нахождение степени, в которую следует возвести простое число для получения заданного целого числа

нахождение степени, в которую следует возвести целое число для получения заданного целого числа

18. Задачей факторизации числа является...

нахождение степени, в которую следует возвести целое число для получения заданного целого числа

нахождение степени, в которую следует возвести простое число для получения заданного целого числа

разложение числа на простые сомножители

19. Что является открытым ключом в алгоритме RSA

(d, f(n))

(d, n)

(e, f(n))

(e, n)

20. Какой алгоритм шифрования относиться к поточным алгоритмам

AES

DES

TEA

RC4

14.1.2. Экзаменационные вопросы

Законодательные и нормативные документы информационной безопасности.

Алгоритмы симметричного шифрования.

Шифрование информации на основе сети Фейштеля.

Режимы выполнения алгоритмов симметричного шифрования.

Потоковое шифрование.

Алгоритмы потокового шифрования.

Криптографические хеш-функции.

Хеш-функции на основе блочных шифров.

Функция хеширования MD4.

Основные теоремы теории чисел.

Наибольший общий делитель. Алгоритмы Евклида.

Односторонняя функция.

Криптография с открытым ключом.

Задача распределения ключей.

Алгоритм Диффи-Хеллмана.

Комбинированная криптосистема.

Электронная цифровая подпись.

Инфраструктура открытых ключей.

Сертификат открытого ключа.

Идентификация, аутентификация, авторизация.

Методы аутентификации, использующие одноразовые и многоразовые пароли.

Методы аутентификации, использующие симметричные и асимметричные алгоритмы.

Биометрическая аутентификация пользователя.

Межсетевые экраны. Функции межсетевых экранов.

Основные типы межсетевых экранов.

Виртуальные частные сети.

14.1.3. Темы контрольных работ

1. Принципы защиты информации.
2. Цели и значение защиты информации.
3. Задачи защиты информации и функции по их реализации.
4. Виды, методы и средства защиты информации.
5. Кадровое и ресурсное обеспечение защиты информации.

Согласована на портале № 32050

6. Источники дестабилизирующего воздействия на информацию.

7. Каналы утечки информации ограниченного доступа.

8. Современные подходы к понятию угрозы защищаемой информации.

9. Объекты защиты информации.

10. Структура системы защиты информации, назначение составных частей системы.

11. Понятие «носитель защищаемой информации». Соотношение между носителем и источником информации.

12. Классификация мероприятий по защите информации, сферы применения организационно-технологических документов и мероприятий.

13. Объекты (предметы) интеллектуальной собственности как составная часть защищаемой информации.

14. Собственники и владельцы информации, отнесенной к служебной и профессиональной тайне.

15. Функции должностных лиц, наделенных полномочиями по отнесению сведений к государственной тайне.

16. Правовые и организационные принципы отнесения информации к защищаемой.

17. Криминалистическая характеристика компьютерной преступности в России.

18. Состав и классификация носителей защищаемой информации.

19. Понятие утечки информации, виды и причины утечки информации.

20. Модели безопасного подключения к Интернет.

14.1.4. Темы опросов на занятиях

Исторические аспекты и современная постановка задач обеспечения информационной безопасности и защиты информации. Основные понятия и определения: конфиденциальность, целостность, доступность, угроза, уязвимость, риски. Основы российского законодательства в сфере защиты информации.

Основные понятия и определения криптографии. Краткая история развития криптологии.

Классификация методов шифрования. Блочные шифры. Алгоритмы блочного шифрования. Вопросы стойкости блочных шифров. Потоковые шифры. Основные понятия. Алгоритмы потокового шифрования.

Основные понятия и определения теории информации. Основные теоремы теории чисел. Дискретные логарифмы в конечном поле. Элементы теории сложности проблем.

Криптография с открытым ключом. Основные способы использования алгоритмов с открытым ключом. Задача распределения ключей. Алгоритмы шифрования с открытым ключом. Криптографические хеш-функции. Электронная цифровая подпись. Основные процедуры цифровой подписи. Алгоритмы электронной цифровой подписи. Сертификат открытого ключа.

Основные понятия и определения. Понятие криптографического протокола. Методы аутентификации на основе паролей. Методы строгой аутентификации. Биометрическая аутентификация пользователя.

Межсетевые экраны. Режимы функционирования межсетевых экранов и их основные компоненты. Основные схемы сетевой защиты на базе межсетевых экранов. Виртуальные защищенные сети. Основы построения виртуальных защищенных сетей.

Вредоносные программы и их классификация. Методы обнаружения и удаления вирусов. Программные закладки и методы защиты от них.

Концепция комплексной защиты информации. Методология создания, организации и обеспечения функционирования систем комплексной защиты информации (КЗИ).

14.1.5. Вопросы на самоподготовку

Блочный шифр BLOWFISH

Блочный шифр RC5

Блочный шифр RC6

Блочный шифр IDEA

14.1.6. Темы лабораторных работ

Классическая криптография

Асимметричное шифрование и электронная цифровая подпись.

Согласована на портале № 32050

Практическое применение криптографии с открытым ключом.

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 проце-

Согласована на портале № 32050

дура оценивания результатов обучения может проводиться в несколько этапов.