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

Защита информации

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки / специальность: **09.03.01 Информатика и вычислительная техника**
Направленность (профиль) / специализация: **Программное обеспечение средств вычислительной техники и автоматизированных систем**
Форма обучения: **очная**
Факультет: **ФСУ, Факультет систем управления**
Кафедра: **АСУ, Кафедра автоматизированных систем управления**
Курс: **4**
Семестр: **8**
Учебный план набора 2018 года

Распределение рабочего времени

№	Виды учебной деятельности	8 семестр	Всего	Единицы
1	Лекции	22	22	часов
2	Практические занятия	12	12	часов
3	Лабораторные работы	20	20	часов
4	Всего аудиторных занятий	54	54	часов
5	Самостоятельная работа	54	54	часов
6	Всего (без экзамена)	108	108	часов
7	Подготовка и сдача экзамена	36	36	часов
8	Общая трудоемкость	144	144	часов
		4.0	4.0	З.Е.

Экзамен: 8 семестр

Томск 2018

Рассмотрена и одобрена на заседании кафедры
протокол № 5 от «26» 4 2018 г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 09.03.01 Информатика и вычислительная техника, утвержденного 12.01.2016 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 ФСУ _____ П. В. Сенченко

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

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 «Защита информации» (Б1.Б.15) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Математика, Программирование, Структуры и алгоритмы обработки данных в ЭВМ.

Последующими дисциплинами являются: Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ОПК-5 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 направления в защите компьютерной информации, принципы защиты информации, принципы классификации и примеры угроз безопасности компьютерным системам, современные подходы к защите продуктов и систем информационных технологий, реализованные в действующих отечественных и международных стандартах ИТ-безопасности, основные инструменты обеспечения многоуровневой безопасности в информационных системах методы и средства обеспечения информационной безопасности компьютерных систем.

– **уметь** выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в ИС, проводить анализ защищенности компьютера и сетевой среды; организовывать безопасную работу в Интернет; использовать средства защиты данных от разрушающих программных воздействий компьютерных вирусов.

– **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 4.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		8 семестр
Аудиторные занятия (всего)	54	54
Лекции	22	22
Практические занятия	12	12
Лабораторные работы	20	20
Самостоятельная работа (всего)	54	54
Оформление отчетов по лабораторным работам	8	8

Проработка лекционного материала	18	18
Самостоятельное изучение тем (вопросов) теоретической части курса	12	12
Подготовка к практическим занятиям, семинарам	16	16
Всего (без экзамена)	108	108
Подготовка и сдача экзамена	36	36
Общая трудоемкость, ч	144	144
Зачетные Единицы	4.0	4.0

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
8 семестр						
1 Введение в информационную безопасность.	2	1	0	4	7	ОПК-5
2 Законодательные и правовые основы защиты компьютерной информации.	2	1	0	4	7	ОПК-5
3 Математические методы и модели в задачах защиты информации.	4	2	8	16	30	ОПК-5
4 Математические основы криптографических методов.	2	2	0	4	8	ОПК-5
5 Криптография с открытым ключом.	2	2	10	6	20	ОПК-5
6 Методы идентификации и аутентификации пользователей.	2	1	0	4	7	ОПК-5
7 Межсетевые экраны и VPN сети.	4	1	0	4	9	ОПК-5
8 Защита компьютерных систем от вредоносных программ.	2	1	0	4	7	ОПК-5
9 Комплексная защита информации.	2	1	2	8	13	ОПК-5
Итого за семестр	22	12	20	54	108	
Итого	22	12	20	54	108	

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

8 семестр			
1 Введение в информационную безопасность.	Исторические аспекты и современная постановка задач обеспечения информационной безопасности (ИБ) и защиты информации, связь проблем ИБ с развитием информационных технологий и процессами глобализации. Основные понятия и определения: конфиденциальность, целостность, доступность, угроза, уязвимость, риски. Обзор и параметры классификации угроз безопасности информации. Принципы защиты информации. Классы средств защиты информации. Государственная стратегия обеспечения ИБ в России.	2	ОПК-5
	Итого	2	
2 Законодательные и правовые основы защиты компьютерной информации.	Основы российского законодательства в сфере защиты информации. Ответственность за правонарушения и преступления в сфере компьютерной информации и защиты информации.Политика безопасности. Модели безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. Стандарты по оценке защищенных систем.	2	ОПК-5
	Итого	2	
3 Математические методы и модели в задачах защиты информации.	Основные понятия и определения криптографии. Краткая история развития криптологии. Методы шифрования. Основные понятия и определения. Классификация методов шифрования. Блочные шифры. Сеть Фейштеля. Алгоритмы блочного шифрования. Режимы выполнения алгоритмов шифрования. Вопросы стойкости блочных шифров. Потоковые шифры. Основные понятия. Алгоритмы потокового шифрования.	4	ОПК-5
	Итого	4	
4 Математические основы криптографических методов.	Основные понятия и определения теории информации. Основные теоремы теории чисел. Дискретные логарифмы в конечном поле. Элементы теории сложности проблем. Классы сложности проблем.	2	ОПК-5
	Итого	2	
5 Криптография с открытым ключом.	Криптография с открытым ключом. Основные способы использования алгоритмов с открытым ключом. Алгоритмы шифрования с открытым ключом. Вопросы стойкости.Задача распределения ключей. Криптографические хеш-функции. Хеш-функции на базе блочных шифров. Электронная цифровая подпись. Общие сведения об электронной цифровой подписи. Основные процедуры цифровой подписи. Алгоритмы электронной цифровой подписи. Вопросы стойкости электронной цифровой подписи. Сертификат открытого ключа.	2	ОПК-5
	Итого	2	

6 Методы идентификации и аутентификации пользователей.	Основные понятия и определения. Понятие криптографического протокола. Методы аутентификации на основе паролей. Методы строгой аутентификации. Биометрическая аутентификация пользователя.	2	ОПК-5
	Итого	2	
7 Межсетевые экраны и VPN сети.	Межсетевые экраны. Режим функционирования межсетевых экранов и их основные компоненты. Основные схемы сетевой защиты на базе межсетевых экранов. Формирование политики межсетевого взаимодействия. Персональные межсетевые экраны.Виртуальные защищенные сети. Концепция построения виртуальных защищенных сетей (VPN). Основные понятия и функции. Достоинства применения технологии VPN.	4	ОПК-5
	Итого	4	
8 Защита компьютерных систем от вредоносных программ.	Вредоносные программы и их классификация. Методы обнаружения и удаления вирусов. Программные закладки и методы защиты от них.	2	ОПК-5
	Итого	2	
9 Комплексная защита информации.	Концепция комплексной защиты информации. Анализ схемы функций защиты и результатов защиты информации. Методология создания, организации и обеспечения функционирования систем комплексной защиты информации (КЗИ). Пути и проблемы практической реализации концепции КЗИ.	2	ОПК-5
	Итого	2	
Итого за семестр		22	

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
Предшествующие дисциплины									
1 Математика			+	+	+	+	+	+	+
2 Программирование			+	+	+	+	+	+	+
3 Структуры и алгоритмы обработки данных в ЭВМ			+	+	+	+	+	+	
Последующие дисциплины									
1 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	+	+	+	+	+	+	+	+	+

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

Компетенции	Виды занятий				Формы контроля
	Лек.	Прак. зан.	Лаб. раб.	Сам. раб.	
ОПК-5	+	+	+	+	Экзамен, Конспект самоподготовки, Защита отчета, 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			
3 Математические методы и модели в задачах защиты информации.	Классическая криптография	4	ОПК-5
	Блочное симметричное шифрование	4	
	Итого	8	
5 Криптография с открытым ключом.	Асимметричное шифрование	4	ОПК-5
	Электронная цифровая подпись	4	
	Практическое применение криптографии с открытым ключом.	2	
	Итого	10	
9 Комплексная защита информации.	Защита информации в операционной системы Windows.	2	ОПК-5
	Итого	2	
Итого за семестр		20	

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

8 семестр			
1 Введение в информационную безопасность.	Федеральный закон «Об информации, информационных технологиях и о защите информации»	1	ОПК-5
	Итого	1	
2 Законодательные и правовые основы защиты компьютерной информации.	Методы оценки уязвимости информации	1	ОПК-5
	Итого	1	
3 Математические методы и модели в задачах защиты информации.	Современные приложения криптографии	2	ОПК-5
	Итого	2	
4 Математические основы криптографических методов.	Сложные математические задачи и алгоритмы ЭЦП	2	ОПК-5
	Итого	2	
5 Криптография с открытым ключом.	Федеральный закон «Об электронной цифровой подписи»	2	ОПК-5
	Итого	2	
6 Методы идентификации и аутентификации пользователей.	Методы аутентификации	1	ОПК-5
	Итого	1	
7 Межсетевые экраны и VPN сети.	Основные технологии построения защищенных информационных систем	1	ОПК-5
	Итого	1	
8 Защита компьютерных систем от вредоносных программ.	Место информационной безопасности информационной системы в национальной безопасности страны. Концепция информационной безопасности.	1	ОПК-5
	Итого	1	
9 Комплексная защита информации.	Комплексная система обеспечения информационной безопасности.	1	ОПК-5
	Итого	1	
Итого за семестр		12	

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
8 семестр				
1 Введение в	Подготовка к практиче-	2	ОПК-5	Опрос на занятиях, Тест,

информационную безопасность.	ским занятиям, семинарам			Экзамен
	Проработка лекционного материала	2		
	Итого	4		
2 Законодательные и правовые основы защиты компьютерной информации.	Подготовка к практическим занятиям, семинарам	2	ОПК-5	Опрос на занятиях, Тест, Экзамен
	Проработка лекционного материала	2		
	Итого	4		
3 Математические методы и модели в задачах защиты информации.	Самостоятельное изучение тем (вопросов) теоретической части курса	12	ОПК-5	Защита отчета, Конспект самоподготовки, Опрос на занятиях, Отчет по лабораторной работе, Тест, Экзамен
	Проработка лекционного материала	2		
	Оформление отчетов по лабораторным работам	2		
	Итого	16		
4 Математические основы криптографических методов.	Подготовка к практическим занятиям, семинарам	2	ОПК-5	Опрос на занятиях, Тест, Экзамен
	Проработка лекционного материала	2		
	Итого	4		
5 Криптография с открытым ключом.	Подготовка к практическим занятиям, семинарам	2	ОПК-5	Защита отчета, Опрос на занятиях, Отчет по лабораторной работе, Тест, Экзамен
	Проработка лекционного материала	2		
	Оформление отчетов по лабораторным работам	2		
	Итого	6		
6 Методы идентификации и аутентификации пользователей.	Подготовка к практическим занятиям, семинарам	2	ОПК-5	Опрос на занятиях, Тест, Экзамен
	Проработка лекционного материала	2		
	Итого	4		
7 Межсетевые экраны и VPN сети.	Подготовка к практическим занятиям, семинарам	2	ОПК-5	Опрос на занятиях, Тест, Экзамен
	Проработка лекционного материала	2		
	Итого	4		

8 Защита компьютерных систем от вредоносных программ.	Подготовка к практическим занятиям, семинарам	2	ОПК-5	Опрос на занятиях, Тест, Экзамен
	Проработка лекционного материала	2		
	Итого	4		
9 Комплексная защита информации.	Подготовка к практическим занятиям, семинарам	2	ОПК-5	Защита отчета, Опрос на занятиях, Отчет по лабораторной работе, Тест, Экзамен
	Проработка лекционного материала	2		
	Оформление отчетов по лабораторным работам	4		
	Итого	8		
Итого за семестр		54		
	Подготовка и сдача экзамена	36		Экзамен
Итого		90		

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
8 семестр				
Защита отчета	4	4	4	12
Конспект самоподготовки	2	2	2	6
Опрос на занятиях	6	6	6	18
Отчет по лабораторной работе	4	8	4	16
Тест	6	6	6	18
Итого максимум за период	22	26	22	70
Экзамен				30
Нарастающим итогом	22	48	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. 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. Партыка Т.Л. Информационная безопасность: Учебное пособие. 3-е изд., исп. и доп. – М.: Форум, 2007. – 367 с. (наличие в библиотеке ТУСУР - 20 экз.)

3. 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.)

4. 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.)

5. 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.)

6. 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.)

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Горитов А.Н. Защита информации: методические указания к практическим занятиям по дисциплине «Защита информации» для направления подготовки 09.03.01 – «Информатика и вычислительная техника». – Томск: ТУСУР, 2016. – 8 с. [Электронный ресурс]. [Электронный ресурс] - Режим доступа: http://asu.tusur.ru/learning/090301/d33/090301-d33-pract.pdf, дата обращения: 16.05.2018.

2. Горитов А.Н. Защита информации: методические указания по выполнению лабораторных работ по дисциплине «Защита информации» для направления подготовки 09.03.01 – «Инфор-

матика и вычислительная техника». – Томск: ТУСУР, 2016. – 6 с. [Электронный ресурс] [Электронный ресурс] - Режим доступа: http://asu.tusur.ru/learning/090301/d33/090301-d33-lab.pdf, дата обращения: 16.05.2018.

3. Горитов А.Н. Защита информации: методические указания по самостоятельной и индивидуальной работе студентов по дисциплине «Защита информации» для направления подготовки 09.03.01 – «Информатика и вычислительная техника». – Томск: ТУСУР, 2016. – 8 с. [Электронный ресурс]. [Электронный ресурс] - Режим доступа: http://asu.tusur.ru/learning/090301/d33/090301-d33-work.pdf, дата обращения: 16.05.2018.

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. 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;
- Рабочее место преподавателя.

Программное обеспечение:

– Far Manager
– LibreOffice
– Microsoft Visual Studio 2013 Professional
– Microsoft Windows 7 Pro
– Notepad++

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:

– Code::Blocks
– Free Pascal
– Lazarus
– LibreOffice
– Microsoft Visual Studio 2013 Professional
– Microsoft Windows 7 Pro
– MySQL Community edition (GPL)
– Notepad++

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.

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 ин-

формационно-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
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...
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 це-

лого 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

1) Законодательные и нормативные документы информационной безопасности.
2) Алгоритмы симметричного шифрования.
3) Шифрование информации на основе сети Фейштеля.
4) Режимы выполнения алгоритмов симметричного шифрования.
5) Потоковое шифрование.
6) Алгоритмы потокового шифрования.
7) Криптографические хеш-функции.
8) Хеш-функции на основе блочных шифров.
9) Функция хеширования MD4.
10) Основные теоремы теории чисел.
11) Наибольший общий делитель. Алгоритмы Евклида.
12) Односторонняя функция.
13) Криптография с открытым ключом.
14) Задача распределения ключей.
15) Алгоритм Диффи-Хеллмана.
16) Комбинированная криптосистема.
17) Электронная цифровая подпись.
18) Инфраструктура открытых ключей.
19) Сертификат открытого ключа.
20) Идентификация, аутентификация, авторизация.
21) Методы аутентификации, использующие одноразовые и многоразовые пароли.
22) Методы аутентификации, использующие симметричные и ассиметричные алгоритмы.
23) Биометрическая аутентификация пользователя.
24) Межсетевые экраны. Функции межсетевых экранов.
25) Основные типы межсетевых экранов.
26) Виртуальные частные сети.

14.1.3. Темы опросов на занятиях

Исторические аспекты и современная постановка задач обеспечения информационной безопасности (ИБ) и защиты информации. Связь проблем ИБ с развитием информационных технологий и процессами глобализации. Основные понятия и определения: конфиденциальность, целостность, доступность, угроза, уязвимость, риски. Принципы защиты информации. Классы средств защиты информации.

Основы российского законодательства в сфере защиты информации. Ответственность за правонарушения и преступления в сфере компьютерной информации и защиты информации. Политика безопасности. Модели безопасности. Критерии и классы защищенности средств вычисли-

тельной техники и автоматизированных информационных систем. Стандарты по оценке защищенных систем.

Основные понятия и определения криптографии. Краткая история развития криптологии.

Методы шифрования. Основные понятия и определения. Классификация методов шифрования. Блочные шифры. Сеть Фейштеля. Алгоритмы блочного шифрования. Режимы выполнения алгоритмов 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. Классы сложности проблем.

Криптография с открытым ключом. Основные способы использования алгоритмов с открытым ключом. Алгоритмы шифрования с открытым ключом. Вопросы стойкости. Задача распределения ключей. Криптографические хеш-функции. Электронная цифровая подпись. Общие сведения об электронной цифровой подписи. Основные процедуры цифровой подписи. Алгоритмы электронной цифровой подписи. Вопросы стойкости 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. Режим функционирования межсетевых экранов и их основные компоненты. Основные схемы сетевой защиты на базе межсетевых экранов. Виртуальные защищенные сети. Концепция построения виртуальных защищенных сетей. Основные понятия и функции.

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

Концепция комплексной защиты информации. Анализ схемы функций защиты и результатов защиты информации. Методология создания, организации и обеспечения функционирования систем комплексной защиты информации (КЗИ). Пути и проблемы практической реализации концепции КЗИ.

14.1.4. Вопросы на самоподготовку

Блочный шифр BLOWFISH
Блочный шифр RC5
Блочный шифр RC6
Блочный шифр IDEA

14.1.5. Темы лабораторных работ

Классическая криптография
Блочное симметричное шифрование
Асимметричное шифрование
Электронная цифровая подпись
Практическое применение криптографии с открытым ключом.
Защита информации в операционной системы Windows.

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.