МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Директор департамента образования
_____ П.Е. Троян
«19» _____12_____ 2018 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 экономике**
Форма обучения: **заочная**
Факультет: **Заочный и вечерний факультет (ЗиВФ)**
Кафедра: **Кафедра автоматизированных систем управления (АСУ)**
Курс: **4**
Семестр: **7, 8**
Учебный план набора 2019 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	7 семестр	8 семестр	Всего	Единицы
Лекционные занятия	2	8	10	часов
Лабораторные занятия	4	8	12	часов
Самостоятельная работа	30	81	111	часов
Контрольные работы		2	2	часов
Подготовка и сдача экзамена		9	9	часов
Общая трудоемкость (включая промежуточную аттестацию)	36	108	144	часов
			4	з.е.

Формы промежуточной аттестация	Семестр	Количество
Экзамен	8	
Контрольные работы	8	1

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Шелупанов А.А.
Должность: Ректор
Дата подписания: 19.12.2018
Уникальный программный ключ:
c53e145e-8b20-45aa-9347-a5e4dbb90e8d

Томск

Согласована на портале № 65976

1. Общие положения

1.1. Цели дисциплины

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

1.2. Задачи дисциплины

1. Овладение теоретическими знаниями в области информационных технологий и обеспечения их безопасности, а также управления информационными ресурсами.
2. Приобретение прикладных знаний в области создания систем защиты информации, а также оптимизации моделей сложных процессов бизнеса.
3. Овладение навыками самостоятельного использования соответствующих инструментальных программных систем.

2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).
Индекс дисциплины: Б1.О.23.
Реализуется с применением электронного обучения, дистанционных образовательных технологий.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой (таблица 3.1):
Таблица 3.1 – Компетенции и индикаторы их достижения

Компетенция	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
Универсальные компетенции		
-	-	-
Общепрофессиональные компетенции		

Согласована на портале № 65976

ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1. Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	В результате изучения дисциплины студент должен знать принципы, методы и средства решения стандартных задач профессиональной деятельности, основы информационной и библиографической культуры, современные информационно-коммуникационные технологии для поиска и анализа информации, основные требования информационной безопасности в профессиональной деятельности
	ОПК-3.2. Умеет 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 студент должен уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
	ОПК-3.3. Владеет навыками подготовки и оформления информационных ресурсов, например, в виде обзоров, рефератов, докладов, с применением современных технологий и с учетом основных требований информационной безопасности	В результате изучения дисциплины студент должен овладеть навыками подготовки и оформления информационных ресурсов с применением современных технологий и с учетом основных требований информационной безопасности
Профессиональные компетенции		
-	-	-

4. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 4 зачетных единиц, 144 академических часов.

Распределение трудоемкости дисциплины по видам учебной деятельности представлено в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины по видам учебной деятельности

Виды учебной деятельности	Всего часов	Семестры	
		7 семестр	8 семестр
Контактная аудиторная работа обучающихся с преподавателем, всего	24	6	18
Лекционные занятия	10	2	8
Лабораторные занятия	12	4	8
Контрольные работы	2		2
Самостоятельная работа обучающихся, в т.ч. контактная внеаудиторная работа обучающихся с преподавателем, всего	111	30	81
Подготовка к тестированию	47	12	35
Подготовка к контрольной работе	56	14	42
Подготовка к лабораторной работе, написание отчета	8	4	4
Подготовка и сдача экзамена	9		9
Общая трудоемкость (в часах)	144	36	108
Общая трудоемкость (в з.е.)	4	1	3

Согласована на портале № 65976

5. Структура и содержание дисциплины

5.1. Разделы (темы) дисциплины и виды учебной деятельности

Структура дисциплины по разделам (темам) и видам учебной деятельности приведена в таблице 5.1.

Таблица 5.1 – Разделы (темы) дисциплины и виды учебной деятельности

Названия разделов (тем) дисциплины	Лек. зан., ч	Лаб. раб.	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
7 семестр					
1 Введение в информационную безопасность	1	4	15	20	ОПК-3
2 Законодательные и правовые основы защиты компьютерной информации	1	-	15	16	ОПК-3
Итого за семестр	2	4	30	36	
8 семестр					
9 Математические методы и модели в задачах защиты информации	1	-	12	15	ОПК-3
10 Математические основы криптографических методов.	2	4	12	18	ОПК-3
11 Криптография с открытым ключом	1	4	12	17	ОПК-3
12 Методы идентификации и аутентификации пользователей.	1	-	12	13	ОПК-3
13 Межсетевые экраны и VPN сети.	1	-	12	13	ОПК-3
14 Защита компьютерных систем от вредоносных программ.	1	-	11	12	ОПК-3
15 Комплексная защита информации.	1	-	10	11	ОПК-3
Итого за семестр	8	8	81	97	
Итого	10	12	111	133	

5.2. Содержание разделов (тем) дисциплины

Содержание разделов (тем) дисциплины (в т.ч. по лекциям) приведено в таблице 5.2.

Таблица 5.2 – Содержание разделов (тем) дисциплины (в т.ч. по лекциям)

Названия разделов (тем) дисциплины	Содержание разделов (тем) дисциплины (в т.ч. по лекциям)	Трудоемкость (лекционные занятия), ч	Формируемые компетенции
7 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. Принципы защиты информации. Классы средств защиты информации.	1	ОПК-3
	Итого	1	

Согласована на портале № 65976

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	1	ОПК-3
	Итого	1	
	Итого за семестр	2	
8 семестр			
9 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	1	ОПК-3
	Итого	1	
10 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-3
	Итого	2	
11 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. 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.	1	ОПК-3
	Итого	1	

Согласована на портале № 65976

12 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-3
	Итого	1	
13 Межсетевые экраны и VPN сети.	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.	1	ОПК-3
	Итого	1	
14 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-3
	Итого	1	
15 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.	1	ОПК-3
	Итого	1	
Итого за семестр		8	
Итого		10	

5.3. Контрольные работы

Виды контрольных работ и часы на контрольные работы приведены в таблице 5.3.

Таблица 5.3 – Контрольные работы

№ п.п.	Виды контрольных работ	Трудоемкость, ч	Формируемые компетенции
8 семестр			
1	Контрольная работа	2	ОПК-3
Итого за семестр		2	
Итого		2	

5.4. Лабораторные занятия

Наименование лабораторных работ приведено в таблице 5.4.

Таблица 5.4 – Наименование лабораторных работ

Названия разделов (тем) дисциплины	Наименование лабораторных работ	Трудоемкость, ч	Формируемые компетенции
7 семестр			

Согласована на портале № 65976

1 Введение в информационную безопасность	Методы донаучной криптографии	4	ОПК-3
	Итого	4	
Итого за семестр		4	
8 семестр			
10 Математические основы криптографических методов.	Электронная цифровая подпись	4	ОПК-3
	Итого	4	
11 Криптография с открытым ключом	Практическое применение криптографии с открытым ключом	4	ОПК-3
	Итого	4	
Итого за семестр		8	
Итого		12	

5.5. Практические занятия (семинары)

Не предусмотрено учебным планом

5.6. Курсовой проект / курсовая работа

Не предусмотрено учебным планом

5.7. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 5.7.

Таблица 5.7 – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов (тем) дисциплины	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
7 семестр				
1 Введение в информационную безопасность	Подготовка к тестированию	5	ОПК-3	Тестирование
	Подготовка к контрольной работе	6	ОПК-3	Контрольная работа
	Подготовка к лабораторной работе, написание отчета	4	ОПК-3	Лабораторная работа
	Итого	15		
2 Законодательные и правовые основы защиты компьютерной информации	Подготовка к тестированию	7	ОПК-3	Тестирование
	Подготовка к контрольной работе	8	ОПК-3	Контрольная работа
	Итого	15		
Итого за семестр		30		
8 семестр				
9 Математические методы и модели в задачах защиты информации	Подготовка к контрольной работе	6	ОПК-3	Контрольная работа
	Подготовка к тестированию	6	ОПК-3	Тестирование
	Итого	12		

Согласована на портале № 65976

10 Математические основы криптографических методов.	Подготовка к контрольной работе	6	ОПК-3	Контрольная работа
	Подготовка к тестированию	4	ОПК-3	Тестирование
	Подготовка к лабораторной работе, написание отчета	2	ОПК-3	Лабораторная работа
	Итого	12		
11 Криптография с открытым ключом	Подготовка к контрольной работе	6	ОПК-3	Контрольная работа
	Подготовка к тестированию	4	ОПК-3	Тестирование
	Подготовка к лабораторной работе, написание отчета	2	ОПК-3	Лабораторная работа
	Итого	12		
12 Методы идентификации и аутентификации пользователей.	Подготовка к контрольной работе	6	ОПК-3	Контрольная работа
	Подготовка к тестированию	6	ОПК-3	Тестирование
	Итого	12		
13 Межсетевые экраны и VPN сети.	Подготовка к контрольной работе	6	ОПК-3	Контрольная работа
	Подготовка к тестированию	6	ОПК-3	Тестирование
	Итого	12		
14 Защита компьютерных систем от вредоносных программ.	Подготовка к контрольной работе	6	ОПК-3	Контрольная работа
	Подготовка к тестированию	5	ОПК-3	Тестирование
	Итого	11		
15 Комплексная защита информации.	Подготовка к контрольной работе	6	ОПК-3	Контрольная работа
	Подготовка к тестированию	4	ОПК-3	Тестирование
	Итого	10		
Итого за семестр		81		
	Подготовка и сдача экзамена	9		Экзамен
Итого		120		

5.8. Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной деятельности

Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной деятельности представлено в таблице 5.8.

Таблица 5.8 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Формируемые компетенции	Виды учебной деятельности			Формы контроля
	Лек. зан.	Лаб. раб.	Сам. раб.	

Согласована на портале № 65976

ОПК-3	+	+	+	Контрольная работа, Лабораторная работа, Тестирование, Экзамен

6. Рейтинговая система для оценки успеваемости обучающихся

Рейтинговая система не используется

7. Учебно-методическое и информационное обеспечение дисциплины

7.1. 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.).

7.2. 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. 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. 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.).

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. Введение в информационную безопасность : учебное пособие / А. А. Малюк, В. С. Горбатов, В. И. Королев [и др.] ; под редакцией В. С. Горбатова. — Москва : Горячая линия-Телеком, 2018. — 288 с. — ISBN 978-5-9912-0160-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111075 [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/111075.

7. Информационная безопасность : учебное пособие / составители Е. Р. Кирколуп [и др.]. — Барнаул : АлтГПУ, 2017. — 316 с. — ISBN 978-5-88210-898-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/112164 [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/112164.

7.3. Учебно-методические пособия

7.3.1. Обязательные учебно-методические пособия

1. Горитов А.Н. Информационная безопасность: Методические указания к лабораторным работам, практическим занятиям и организации самостоятельной работы для студентов направления «Прикладная информатика» (уровень бакалавриата) заочной формы обучения. – Томск: ТУСУР, 2018. – 15 с. [Электронный ресурс]: — Режим доступа: https://asu.tusur.ru/learning/090303/d40/090303-d40-lab.pdf.

7.3.2. 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;

Согласована на портале № 65976

– в печатной форме.

7.4. Современные профессиональные базы данных и информационные справочные системы

1. При изучении дисциплины рекомендуется обращаться к современным базам данных, информационно-справочным и поисковым системам, к которым у ТУСУРа открыт доступ: https://lib.tusur.ru/ru/resursy/bazy-dannyh.

8. Материально-техническое и программное обеспечение дисциплины

8.1. 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 достаточным количеством посадочных мест для учебной группы, оборудованная доской и стандартной учебной мебелью. Имеются мультимедийное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

8.2. Материально-техническое и программное обеспечение для лабораторных работ

Учебная вычислительная лаборатория / Лаборатория ГПО "Алгоритм": 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, 439 ауд.

Описание имеющегося оборудования:
- Рабочие станции Intel Celeron 1.7 (10 шт.);
- Проектор Acer X125H DLP;
- Экран проектора;
- Видеокамера (2 шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:
- 7-Zip;
- Code::Blocks;
- Far Manager;
- Free Pascal;
- Lazarus;
- LibreOffice;
- Microsoft PowerPoint Viewer;
- Microsoft Visual Studio 2013 Professional;
- Microsoft Windows 7 Pro;
- Notepad++;

8.3. 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, 209 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Описание имеющегося оборудования:
- учебная мебель;
- компьютеры;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду ТУСУРа.

Перечень программного обеспечения:

Согласована на портале № 65976

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

8.4. 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 зрения** 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.

9. Оценочные материалы и методические рекомендации по организации изучения дисциплины

9.1. Содержание оценочных материалов для текущего контроля и промежуточной аттестации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы, представленные в таблице 9.1.

Таблица 9.1 – Формы контроля и оценочные материалы

Названия разделов (тем) дисциплины	Формируемые компетенции	Формы контроля	Оценочные материалы (ОМ)
1 Введение в информационную безопасность	ОПК-3	Контрольная работа	Примерный перечень вариантов (заданий) контрольных работ
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
2 Законодательные и правовые основы защиты компьютерной информации	ОПК-3	Контрольная работа	Примерный перечень вариантов (заданий) контрольных работ
		Тестирование	Примерный перечень тестовых заданий
9 Математические методы и модели в задачах защиты информации	ОПК-3	Контрольная работа	Примерный перечень вариантов (заданий) контрольных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов

Согласована на портале № 65976

10 Математические основы криптографических методов.	ОПК-3	Контрольная работа	Примерный перечень вариантов (заданий) контрольных работ
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
11 Криптография с открытым ключом	ОПК-3	Контрольная работа	Примерный перечень вариантов (заданий) контрольных работ
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
12 Методы идентификации и аутентификации пользователей.	ОПК-3	Контрольная работа	Примерный перечень вариантов (заданий) контрольных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
13 Межсетевые экраны и VPN сети.	ОПК-3	Контрольная работа	Примерный перечень вариантов (заданий) контрольных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
14 Защита компьютерных систем от вредоносных программ.	ОПК-3	Контрольная работа	Примерный перечень вариантов (заданий) контрольных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
15 Комплексная защита информации.	ОПК-3	Контрольная работа	Примерный перечень вариантов (заданий) контрольных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов

Шкала оценки сформированности отдельных планируемых результатов обучения по дисциплине приведена в таблице 9.2.

Согласована на портале № 65976

Таблица 9.2 – Шкала оценки сформированности планируемых результатов обучения по дисциплине

Оценка	Баллы за ОМ	Формулировка требований к степени сформированности планируемых результатов обучения		
		знать	уметь	владеть
2 (неудовлетворительно)	< 60% от максимальной суммы баллов	отсутствие знаний или фрагментарные знания	отсутствие умений или частично освоенное умение	отсутствие навыков или фрагментарные применение навыков
3 (удовлетворительно)	от 60% до 69% от максимальной суммы баллов	общие, но не структурированные знания	в целом успешно, но не систематически осуществляемое умение	в целом успешное, но не систематическое применение навыков
4 (хорошо)	от 70% до 89% от максимальной суммы баллов	сформированные, но содержащие отдельные проблемы знания	в целом успешное, но содержащие отдельные пробелы умение	в целом успешное, но содержащие отдельные пробелы применение навыков
5 (отлично)	≥ 90% от максимальной суммы баллов	сформированные систематические знания	сформированное умение	успешное и систематическое применение навыков

Шкала комплексной оценки сформированности компетенций приведена в таблице 9.3.

Таблица 9.3 – Шкала комплексной оценки сформированности компетенций

Оценка	Формулировка требований к степени компетенции
2 (неудовлетворительно)	Не имеет необходимых представлений о проверяемом материале или Знать на уровне **ориентирования**, представлений. Обучающийся знает основные признаки или термины изучаемого элемента содержания, их отнесенность к определенной науке, отрасли или объектам, узнает в текстах, изображениях или схемах и знает, к каким источникам нужно обращаться для более детального его усвоения.
3 (удовлетворительно)	Знать и уметь на **репродуктивном** уровне. Обучающихся знает изученный элемент содержания репродуктивно: произвольно воспроизводит свои знания устно, письменно или в демонстрируемых действиях.
4 (хорошо)	Знать, уметь, владеть на **аналитическом** уровне. Зная на репродуктивном уровне, указывать на особенности и взаимосвязи изученных объектов, на их достоинства, ограничения, историю и перспективы развития и особенности для разных объектов усвоения.
5 (отлично)	Знать, уметь, владеть на **системном** уровне. Обучающийся знает изученный элемент содержания системно, произвольно и доказательно воспроизводит свои знания устно, письменно или в демонстрируемых действиях, учитывая и указывая связи и зависимости между этим элементом и другими элементами содержания дисциплины, его значимость в содержании дисциплины.

Согласована на портале № 65976

9.1.1. Примерный перечень тестовых заданий

1. Какие виды алгоритмов подразделяются на блочные и поточные
    1. комбинированные
    2. асимметричные
    3. симметричные
2. Для передачи больших сообщений лучше всего соответствуют режимы:
    1. ECB
    2. CFB
    3. OFB
    4. CBC
3. Режим CBC используется для того, чтобы
    1. увеличить скорость шифрования
    2. не было необходимости разбивать сообщение на целое число блоков достаточно большой длины
    3. одинаковые незашифрованные блоки преобразовывались в различные зашифрованные блоки
4. Хеш-функции предназначены для
    1. сжатия сообщения
    2. шифрования сообщения
    3. получения дайджеста сообщения
5. Алгоритм Диффи-Хеллмана основан на
    1. задаче факторизации числа
    2. задаче определения, является ли данное число простым
    3. задаче дискретного логарифмирования
6. Алгоритм RSA основан на:
    1. задаче дискретного логарифмирования
    2. задаче определения, является ли данное число простым
    3. задаче факторизации числа
7. Цифровая подпись вычисляется:
    1. для отправляемого электронного сообщения
    2. для отправляемого сообщения совместно с дайджестом
    3. для отправляемого сообщения и адресом отправителя
    4. для дайджеста отправляемого электронного сообщения
8. Для создания подписи следует использовать
    1. закрытый ключ получателя
    2. свой открытый ключ
    3. свой закрытый ключ
9. В DSS используется следующая хеш-функция
    1. MD5
    2. SHA-2
    3. SHA-1
10. В стандарте ГОСТ 3410 используется следующая хеш-функция
    1. MD5
    2. SHA-1
    3. ГОСТ 3411

9.1.2. Перечень экзаменационных вопросов

1. Законодательные и нормативные документы информационной безопасности.
2. Алгоритмы симметричного шифрования.
3. Режимы выполнения алгоритмов симметричного шифрования.
4. Потоковое шифрование.
5. Алгоритмы потокового шифрования.
6. Криптографические хеш-функции.
7. Задача распределения ключей.
8. Электронная цифровая подпись.
9. Инфраструктура открытых ключей.

Согласована на портале № 65976

10. Методы биометрической аутентификация пользователя.

9.1.3. Примерный перечень вариантов (заданий) контрольных работ

1. Использование алгоритма RSA при обмене сообщениями двух пользователей.
2. Использование алгоритма Шамира при обмене сообщениями двух пользователей.
3. Использование алгоритма Эль-Гамаля при обмене сообщениями двух пользователей.
4. Использование алгоритма DSS для создания ЭЦП при обмене сообщениями двух пользователей.
5. Использование алгоритма ГОСТ Р 3410-94 для создания ЭЦП при обмене сообщениями двух пользователей.

9.1.4. Темы лабораторных работ

1. Методы донаучной криптографии
2. Электронная цифровая подпись
3. Практическое применение криптографии с открытым ключом

9.2. Методические рекомендации

Учебный материал излагается в форме, предполагающей самостоятельное мышление студентов, самообразование. При этом самостоятельная работа студентов играет решающую роль в ходе всего учебного процесса.

Начать изучение дисциплины необходимо со знакомства с рабочей программой, списком учебно-методического и программного обеспечения. Самостоятельная работа студента включает работу с учебными материалами, выполнение контрольных мероприятий, предусмотренных учебным планом.

В процессе изучения дисциплины для лучшего освоения материала необходимо регулярно обращаться к рекомендуемой литературе и источникам, указанным в учебных материалах; пользоваться через кабинет студента на сайте Университета образовательными ресурсами электронно-библиотечной системы, а также общедоступными интернет-порталами, содержащими научно-популярные и специализированные материалы, посвященные различным аспектам учебной дисциплины.

При самостоятельном изучении тем следуйте рекомендациям:

– чтение или просмотр материала осуществляйте со скоростью, достаточной для индивидуального понимания и освоения материала, выделяя основные идеи; на основании изученного составить тезисы. Освоив материал, попытаться соотнести теорию с примерами из практики;

– если в тексте встречаются незнакомые или малознакомые термины, следует выяснить их значение для понимания дальнейшего материала;

– осмысливайте прочитанное и изученное, отвечайте на предложенные вопросы.

Студенты могут получать индивидуальные консультации, в т.ч. с использованием средств телекоммуникации.

По дисциплине могут проводиться дополнительные занятия, в т.ч. в форме вебинаров. Расписание вебинаров и записи вебинаров публикуются в электронном курсе / электронном журнале по дисциплине.

9.3. 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 9.2.

Таблица 9.2 – 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

Согласована на портале № 65976

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, определяющимися исходя из состояния обучающегося на момент проверки

9.4. 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.

Согласована на портале № 65976

ЛИСТ СОГЛАСОВАНИЯ

Рассмотрена и одобрена на заседании кафедры АСУ
протокол № 13 от «22» 11 2018 г.

СОГЛАСОВАНО:

Должность	Инициалы, фамилия	Подпись
Заведующий выпускающей каф. АСУ	А.М. Кориков	Согласовано, 9e8ba22e-f8dc-42a7-a705-2441d49ffeee
Заведующий обеспечивающей каф. АСУ	А.М. Кориков	Согласовано, 9e8ba22e-f8dc-42a7-a705-2441d49ffeee
Начальник учебного управления	Е.В. Саврук	Согласовано, fa63922b-1fce-4a6a-845d-9ce7670b004c
Декан ЗиВФ	И.В. Осипов	Согласовано, 126832c4-9aa6-45bd-8e71-e9e09d25d010

ЭКСПЕРТЫ:

Доцент, каф. АСУ	А.И. Исакова	Согласовано, 79bf1038-9d22-4279-a1e8-7806307b7f82
Заведующий кафедрой, каф. АСУ	В.В. Романенко	Согласовано, c3e2018f-3231-48c3-b093-89b6f5342191

РАЗРАБОТАНО:

Профессор, каф. АСУ	А.Н. Горитов	Разработано, 1fee132a-a2cd-4e8d-bdd5-8e7aa16d873b

Согласована на портале № 65976