МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Проректор по УР

Документ подписан электронной подписью
Сертификат: a1119608-cdff-4455-b54e-5235117c185c
Владелец: Сенченко Павел Васильевич
Действителен: с 17.09.2019 по 16.09.2024

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

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: **заочная (в том числе с применением дистанционных образовательных технологий)**
Кафедра: **автоматизированных систем управления (АСУ)**
Курс: **4**
Семестр: **8**
Учебный план набора 2024 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	8 семестр	Всего	Единицы
Лабораторные занятия	16	16	часов
Самостоятельная работа	109	109	часов
Самостоятельная работа под руководством преподавателя	8	8	часов
Контрольные работы	2	2	часов
Подготовка и сдача экзамена	9	9	часов
Общая трудоемкость (включая промежуточную аттестацию)	144	144	часов
		4	з.е.

Формы промежуточной аттестации	Семестр	Количество
Экзамен	8	
Контрольные работы	8	1

Томск

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).
Часть блока дисциплин: Обязательная часть.
Модуль дисциплин: Модуль направленности (профиля) (major).
Индекс дисциплины: Б1.О.05.03.
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		

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, основы информационной и библиографической культуры, современные информационно-коммуникационные технологии для поиска и анализа информации, основные требования информационной безопасности в профессиональной деятельности	Знает 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	Умеет 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 по вопросам профессиональной деятельности, с применением современных технологий и с учетом основных требований информационной безопасности	Владеет 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
		8 семестр
Контактная работа обучающихся с преподавателем, всего	26	26
Лабораторные занятия	16	16
Самостоятельная работа под руководством преподавателя	8	8
Контрольные работы	2	2
Самостоятельная работа обучающихся, всего	109	109
Самостоятельное изучение тем (вопросов) теоретической части дисциплины	77	77
Подготовка к контрольной работе	16	16
Подготовка к лабораторной работе	8	8
Написание отчета по лабораторной работе	8	8

Подготовка и сдача экзамена	9	9
Общая трудоемкость (в часах)	144	144
Общая трудоемкость (в з.е.)	4	4

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	Лаб. раб.	Контр. раб.	СРП, ч.	Сам. раб., ч	Всего часов (без промежуточной аттестации)	Формируемые компетенции
8 семестр						
1 Проблемы и методы защиты компьютерной информации.	-	2	1	9	12	ОПК-3
2 Исторические шифры.	-		1	12	13	ОПК-3
3 Основные понятия криптографии.	4		1	16	21	ОПК-3
4 Математические основы криптографических методов.	-		1	12	13	ОПК-3
5 Компьютерные алгоритмы шифрования.	4		1	16	21	ОПК-3
6 Компьютерная безопасность и практическое применение криптографии.	4		1	16	21	ОПК-3
7 Вирусы и угрозы, связанные с вирусами.	-		1	12	13	ОПК-3
8 Брандмауэры.	4		1	16	21	ОПК-3
Итого за семестр	16	2	8	109	135	
Итого	16	2	8	109	135	

5.2. Содержание разделов (тем) дисциплины

Содержание разделов (тем) дисциплины приведено в таблице 5.2.

Таблица 5.2 – Содержание разделов (тем) дисциплины

Названия разделов (тем) дисциплины	Содержание разделов (тем) дисциплины	СРП, ч	Формируемые компетенции
8 семестр			
1 Проблемы и методы защиты компьютерной информации.	Информационная безопасность. Проблемы защиты информации в компьютерных системах. Традиционные вопросы криптографии. Современные приложения криптографии. Понятие криптографического протокола. Криптография и стеганография.	1	ОПК-3
	Итого	1	

2 Исторические шифры.	Подстановочные и перестановочные шифры. Статистические свойства языка шифрования. Шифр сдвига. Шифр замены. Шифр Виженера. Перестановочные шифры. Критерий статистической оценки происхождения шифротекста. Одноразовые блокноты.	1	ОПК-3
	Итого	1	
3 Основные понятия криптографии.	Криптографическая терминология. Алгоритмы и ключи. Однонаправленные функции. Однонаправленная хэш-функция. Передача информации с использованием криптографии с открытыми ключами. Смешанные криптосистемы. Основные протоколы.	1	ОПК-3
	Итого	1	
4 Математические основы криптографических методов.	Теория информации. Теория сложности. Теория чисел. Генерация простого числа. Дискретные логарифмы в конечном поле.	1	ОПК-3
	Итого	1	
5 Компьютерные алгоритмы шифрования.	Симметричные шифры. Поточные шифры. Блочные шифры. Шифр Фейстеля. Шифр DES. Режимы работы DES. Шифр Rijndael. Алгоритм криптографического преобразования ГОСТ 28147-89. Стандарт симметричного шифрования данных IDEA. Однонаправленная хэш-функция MD5. Асимметричный алгоритм шифрования данных RSA. Комплекс криптографических алгоритмов PGP.	1	ОПК-3
	Итого	1	
6 Компьютерная безопасность и практическое применение криптографии.	Общие сведения. Обзор стандартов в области защиты информации. Подсистема информационной безопасности. Защита локальной рабочей станции. Методы и средства обеспечения информационной безопасности локальных рабочих станций. Защита в локальных сетях.	1	ОПК-3
	Итого	1	
7 Вирусы и угрозы, связанные с вирусами.	Вредоносные программы. Лазейки. Логическая бомба. "Троянские кони". Вирус. "Черви". Бактерии. Природа вирусов. Структура вируса. Начальное инфицирование. Типы вирусов. Макровирусы. Антивирусная защита. Перспективные методы антивирусной защиты.	1	ОПК-3
	Итого	1	
8 Брандмауэры.	Принципы разработки брандмауэров. Характеристики брандмауэров. Типы брандмауэров. Конфигурации брандмауэров. Высоконадежные системы.	1	ОПК-3
	Итого	1	
Итого за семестр		8	
Итого		8	

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 с автоматизированной проверкой	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
8 семестр			
3 Основные понятия криптографии.	Администрирование учетных записей пользователей.	4	ОПК-3
	Итого	4	
5 Компьютерные алгоритмы шифрования.	Управление параметрами операционной системы.	4	ОПК-3
	Итого	4	
6 Компьютерная безопасность и практическое применение криптографии.	Дискреционный механизм разграничения доступа.	4	ОПК-3
	Итого	4	
8 Брандмауэры.	Политика ограниченного использования программ.	4	ОПК-3
	Итого	4	
	Итого за семестр	16	
	Итого	16	

5.5. Практические занятия (семинары)

Не предусмотрено учебным планом

5.6. Контроль самостоятельной работы (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
8 семестр				

1 Проблемы и методы защиты компьютерной информации.	Самостоятельное изучение тем (вопросов) теоретической части дисциплины	7	ОПК-3	Тестирование, Экзамен
	Подготовка к контрольной работе	2	ОПК-3	Контрольная работа
	Итого	9		
2 Исторические шифры.	Самостоятельное изучение тем (вопросов) теоретической части дисциплины	10	ОПК-3	Тестирование, Экзамен
	Подготовка к контрольной работе	2	ОПК-3	Контрольная работа
	Итого	12		
3 Основные понятия криптографии.	Подготовка к лабораторной работе	2	ОПК-3	Лабораторная работа
	Написание отчета по лабораторной работе	2	ОПК-3	Отчет по лабораторной работе
	Самостоятельное изучение тем (вопросов) теоретической части дисциплины	10	ОПК-3	Тестирование, Экзамен
	Подготовка к контрольной работе	2	ОПК-3	Контрольная работа
	Итого	16		
4 Математические основы криптографических методов.	Самостоятельное изучение тем (вопросов) теоретической части дисциплины	10	ОПК-3	Тестирование, Экзамен
	Подготовка к контрольной работе	2	ОПК-3	Контрольная работа
	Итого	12		

5 Компьютерные алгоритмы шифрования.	Подготовка к лабораторной работе	2	ОПК-3	Лабораторная работа
	Написание отчета по лабораторной работе	2	ОПК-3	Отчет по лабораторной работе
	Самостоятельное изучение тем (вопросов) теоретической части дисциплины	10	ОПК-3	Тестирование, Экзамен
	Подготовка к контрольной работе	2	ОПК-3	Контрольная работа
	Итого	16		
6 Компьютерная безопасность и практическое применение криптографии.	Подготовка к лабораторной работе	2	ОПК-3	Лабораторная работа
	Написание отчета по лабораторной работе	2	ОПК-3	Отчет по лабораторной работе
	Самостоятельное изучение тем (вопросов) теоретической части дисциплины	10	ОПК-3	Тестирование, Экзамен
	Подготовка к контрольной работе	2	ОПК-3	Контрольная работа
	Итого	16		
7 Вирусы и угрозы, связанные с вирусами.	Самостоятельное изучение тем (вопросов) теоретической части дисциплины	10	ОПК-3	Тестирование, Экзамен
	Подготовка к контрольной работе	2	ОПК-3	Контрольная работа
	Итого	12		
8 Брандмауэры.	Подготовка к лабораторной работе	2	ОПК-3	Лабораторная работа
	Написание отчета по лабораторной работе	2	ОПК-3	Отчет по лабораторной работе
	Самостоятельное изучение тем (вопросов) теоретической части дисциплины	10	ОПК-3	Тестирование, Экзамен
	Подготовка к контрольной работе	2	ОПК-3	Контрольная работа
	Итого	16		
Итого за семестр		109		

	Подготовка и сдача экзамена	9		Экзамен
	Итого	118		

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 учебной деятельности

Формируемые компетенции	Виды учебной деятельности				Формы контроля
	Лаб. раб.	Конт.Раб.	СРП	Сам. раб.	
ОПК-3	+	+	+	+	Контрольная работа, Лабораторная работа, Отчет по лабораторной работе, 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. Спицын В. Г. Информационная безопасность вычислительной техники: Учебное пособие / Спицын В. Г. - Томск: Эль Контент, 2011. - 148 с. Доступ из личного кабинета студента. [Электронный ресурс]: — Режим доступа: https://study.tusur.ru/study/library.

7.2. Дополнительная литература

1. Зайцев, А.П. Технические средства и методы защиты информации: учебное пособие / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков, И.В. Голубятников. — Электрон. дан. — Москва : Горячая линия-Телеком, 2012. — 616 с. — Доступ из личного кабинета студента. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/5154.

2. Шаньгин, В.Ф. Защита компьютерной информации: учебное пособие / В.Ф. Шаньгин. — Электрон. дан. — Москва : ДМК Пресс, 2010. — 544 с. — Доступ из личного кабинета студента. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/1122.

7.3. Учебно-методические пособия

7.3.1. Обязательные учебно-методические пособия

1. Якимук А. Ю. Защита информации. Методические указания по выполнению лабораторной работы: Методические указания / Якимук А. Ю., Конев А. А. - Томск : ФДО, ТУСУР, 2017. – 81 с. Доступ из личного кабинета студента. [Электронный ресурс]: — Режим доступа: https://study.tusur.ru/study/library.

2. Костюченко Е. Ю. Основы информационной безопасности. Методические указания по организации самостоятельной работы: Методические указания / Костюченко Е. Ю., Шелупанов А. А. - Томск : ФДО, ТУСУР, 2018. – 22 с. Доступ из личного кабинета студента. [Электронный ресурс]: — Режим доступа: https://study.tusur.ru/study/library.

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

Учебно-методические материалы для самостоятельной 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.

7.4. Иное учебно-методическое обеспечение

1. Спицин В.Г. Информационная безопасность вычислительной техники [Электронный ресурс]: Электронный курс /В.Г. Спицин. - Томск: ТУСУР ФДО, 2018. (доступ из личного кабинета студента) .

7.5. Современные профессиональные базы данных и информационные справочные системы

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. Общие требования к материально-техническому и программному обеспечению дисциплины

Учебные аудитории для проведения занятий лабораторного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, для самостоятельной работы студентов

634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Описание имеющегося оборудования:

- Веб-камера - 6 шт.;
- Наушники с микрофоном - 6 шт.;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- 7-Zip;
- Google Chrome;
- Kaspersky Endpoint Security для Windows;
- LibreOffice;
- Microsoft Windows;

8.2. 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:

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

- Google Chrome.

8.3. 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 Проблемы и методы защиты компьютерной информации.	ОПК-3	Контрольная работа	Примерный перечень вариантов (заданий) контрольных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
2 Исторические шифры.	ОПК-3	Контрольная работа	Примерный перечень вариантов (заданий) контрольных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов

3 Основные понятия криптографии.	ОПК-3	Контрольная работа	Примерный перечень вариантов (заданий) контрольных работ
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по лабораторной работе	Темы лабораторных работ
4 Математические основы криптографических методов.	ОПК-3	Контрольная работа	Примерный перечень вариантов (заданий) контрольных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
5 Компьютерные алгоритмы шифрования.	ОПК-3	Контрольная работа	Примерный перечень вариантов (заданий) контрольных работ
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по лабораторной работе	Темы лабораторных работ
6 Компьютерная безопасность и практическое применение криптографии.	ОПК-3	Контрольная работа	Примерный перечень вариантов (заданий) контрольных работ
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по лабораторной работе	Темы лабораторных работ

7 Вирусы и угрозы, связанные с вирусами.	ОПК-3	Контрольная работа	Примерный перечень вариантов (заданий) контрольных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
8 Брандмауэры.	ОПК-3	Контрольная работа	Примерный перечень вариантов (заданий) контрольных работ
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по лабораторной работе	Темы лабораторных работ

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

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.

9.1.1. Примерный перечень тестовых заданий

1. Количество знаков в шифротексте и в исходном тексте в общем случае:
    1. не может различаться.
    2. может различаться.
    3. должно быть равно сумме знаков открытого текста и ключа.
    4. должно быть равно разности знаков открытого текста и ключа.
    5. должно быть равно длине алфавита.
2. Все элементы систем защиты подразделяются на две категории – долговременные и легкозаменяемые. К долговременным элементам относятся:
    1. секретный ключ.
    2. алгоритм шифрования.
    3. открытый ключ.
    4. пароль.
    5. идентификатор данных.
3. Стойкость современных криптосистем основывается на:
    1. секретности долговременных элементов криптозащиты.
    2. применении стеганографических алгоритмов.
    3. секретности алгоритма шифрования.
    4. секретности информации сравнительно малого размера, называемой ключом.
    5. секретности алгоритма шифрования и ключа.
4. Подстановочным шифром называется шифр, в котором:
    1. используется матрица чисел размерностью 5x5.
    2. используется открытый ключ.
    3. используется фрагмент текста.
    4. используется фрагмент текста и открытый ключ.
    5. каждый символ открытого текста в шифротексте заменяется другим символом.
5. Перестановочный шифр в отличие от подстановочного:
    1. является более стойким.
    2. использует открытый ключ.
    3. имеет больший период.
    4. использует множественные ключи.

5. меняет не открытый текст, а порядок символов.

6. В однозвучном подстановочном шифре:
    1. один символ открытого текста отображается на несколько символов шифротекста.
    2. два символа открытого текста отображаются на один символ шифротекста.
    3. три символа открытого текста отображаются на один символ шифротекста.
    4. четыре символа открытого текста отображаются на один символ шифротекста.
    5. пять символов открытого текста отображаются на один символ шифротекста.
7. Открытый текст M (message) для компьютера – это
    1. двоичные данные.
    2. набор символов.
    3. текстовый файл.
    4. оцифрованный звук.
    5. цифровое видеоизображение.
8. Энтропия сообщения в теории информации определяет:
    1. число символов в сообщении.
    2. норму языка.
    3. количество возможных значений сообщения.
    4. размер ключа.
    5. вероятность появления тех или иных символов.
9. Работа симметричных шифров включает в себя два преобразования:
   C = Ek(m) и m = Dk(C), где m – открытый текст, E – шифрующая функция, D – расшифровывающая функция, C – шифротекст, k–
    1. пространство ключей.
    2. секретный ключ.
    3. число символов в алфавите.
    4. порядковый номер шифрующей и дешифрующей функций.
    5. длина открытого текста.
10. Функция шифрования E(M) = C открытого текста M в шифротекст C создает на выходе для компьютера:
    1. закодированный набор символов.
    2. текстовый файл того же размера, что и M.
    3. текстовый файл большего размера, чем M.
    4. текстовый файл меньшего размера, чем M.
    5. двоичные данные.
11. Криптостойкость симметричных шифров зависит только от секретности используемого ключа. Ключ, исключающий взлом простым перебором, содержит не менее чем:
    1. 64 бита.
    2. 80 бит.
    3. 48 бит.
    4. 32 бита.
    5. 16 бит.
12. Идентичность понятий “криптографический алгоритм” и “шифр” позволяют определить криптосистему, как совокупность:
    1. математических функций, используемых для шифрования и дешифрования.
    2. шифра, открытого текста и шифротекста.
    3. шифра и пространства ключей.
    4. математических функций, используемых для шифрования и дешифрования, пространства ключей и открытого текста.
    5. шифра, всевозможных открытых текстов, шифротекстов и ключей.
13. В большинстве симметричных алгоритмов ключ шифрования:
    1. совпадает с ключом дешифрования.
    2. не может быть рассчитан по ключу дешифрования.
    3. применяется в совокупности с несколькими ключами.
    4. является открытым.
    5. чаще всего хранится в некоторой базе данных.
14. В общем случае энтропия сообщения – это:

1. число символов в сообщении.
2. количество символов, необходимых для кодирования сообщения.
3. минимальное количество бит, необходимых для кодирования всех возможных значений сообщения.
4. длина сообщения в битах.
5. вероятность появления тех или иных символов.

15. Для обеспечения безопасной передачи данных по сети на физическом и канальном уровнях применяются следующие подходы:
    1. аутентификация рабочей станции, являющейся источником сообщений.
    2. административная защита на маршрутизаторах.
    3. шифрование соединения.
    4. выборочное или полное шифрование трафика.
    5. фильтрация трафика между внутренней сетью и внешней коммуникационной средой.
    6. защита при помощи межсетевых экранов.
16. К вредоносным программам, требующим программу-носитель, относятся:
    1. бактерии.
    2. логические бомбы.
    3. «троянские кони».
    4. черви.
    5. вирусы.
17. Укажите высказывания, которые верны по отношению к лазейкам:
    1. лазейки относятся к вредоносным программам, не требующим программы-носителя.
    2. лазейка — это секретная точка входа в программу, позволяющая тому, кто знает о ее существовании, получить доступ в обход стандартных процедур защиты.
    3. контроль возможных лазеек легко реализуется стандартными средствами операционной системы.
    4. лазейки незаконно используются в программистской практике для ускорения отладки и тестирования программ.
    5. меры защиты от лазеек должны быть сфокусированы на контроле процесса разработки программного обеспечения и его обновления.
18. Какие угрозы можно выделить на двух нижних уровнях модели сетевого взаимодействия?
    1. физическое уничтожение канала связи.
    2. ошибочная коммутация.
    3. атаки на систему маршрутизации.
    4. разведка имен и паролей пользователей.
    5. атаки на систему разграничения прав доступа пользователей.
19. Брандмауэры могут быть:
    1. эффективным средством защиты только локальной рабочей станции, но не компьютерной сети, от угроз, имеющих сетевую природу, в то же время не ограничивающим связь с внешним миром через глобальные сети и Internet.
    2. неэффективным средством защиты локальной системы или компьютерной сети от угроз, имеющих сетевую природу, в то же время не ограничивающим связь с внешним миром через глобальные сети и Internet.
    3. эффективным средством защиты локальной системы или компьютерной сети от угроз, имеющих сетевую природу, в то же время ограничивающим связь с внешним миром через глобальные сети и Internet.
    4. эффективным средством защиты локальной системы или компьютерной сети от угроз, не имеющих сетевую природу, в то же время не ограничивающим связь с внешним миром через глобальные сети и Internet.
    5. эффективным средством защиты локальной системы или компьютерной сети от угроз, имеющих сетевую природу, в то же время не ограничивающим связь с внешним миром через глобальные сети и Internet.
20. Укажите верные утверждения о фильтрующих маршрутизаторах:
    1. Фильтрующий маршрутизатор принимает решение о том, передавать по сети поступивший пакет IP дальше или отвергнуть его, на основе определенного

набора правил.
2. Правила фильтрования основываются на значениях полей заголовка IP, заголовка транспортного уровня, а также номера порта, определяющего приложение.
3. Фильтрующий маршрутизатор работает как ретранслятор данных уровня приложений.
4. Вне зависимости от настроек фильтрующего маршрутизатора, используемая по умолчанию политика – “Все, что не разрешено, запрещено”.
5. Вне зависимости от настроек фильтрующего маршрутизатора, используемая по умолчанию политика – “Все, что не запрещено, разрешено”.

9.1.2. Перечень экзаменационных вопросов

Приведены примеры типовых заданий из банка экзаменационных тестов, составленных по пройденным разделам дисциплины.

1. Шифротекст и исходный текст могут иметь в общем случае:
    1. одинаковое количество знаков.
    2. знаки ключа шифрования.
    3. одинаковое количество знаков и повторяющиеся знаки.
    4. разное количество знаков и повторяющиеся знаки.
    5. ни одного повторяющегося знака.
2. Основным условием стойкости современных криптосистем является секретность:
    1. всех долговременных элементов криптозащиты.
    2. всех легкозаменяемых элементов криптозащиты.
    3. алгоритма шифрования.
    4. информации сравнительно малого размера, называемой ключом.
    5. алгоритма шифрования и ключа.
3. Подстановочный шифр, в котором один символ открытого текста отображается на несколько символов шифротекста, называется:
    1. однозвучным.
    2. моноалфавитным.
    3. полиграмным.
    4. полиалфавитным.
    5. книжным.
4. Подстановочный шифр, который блоки символов шифрует по группам, называется:
    1. однозвучным.
    2. моноалфавитным.
    3. полиграмным.
    4. полиалфавитным.
    5. книжным.
5. Соотношение H (M)=log2 n, где n – количество возможных значений, определяет:
    1. меру избыточности сообщения.
    2. информативность сообщения.
    3. максимум энтропии отдельного символа.
    4. энтропию криптосистемы.
    5. энтропию сообщения.
6. Абсолютная норма языка является функцией:
    1. нормы языка.
    2. числа символов в алфавите.
    3. избыточности языка.
    4. длины сообщения.
    5. энтропии криптосистемы.
7. Для простейшего поточного шифра, использующего в качестве функций шифрования и дешифрования операцию исключающего ИЛИ, при значении открытого текста = 1110101110, потоке ключей = 1010010001, шифротекст =
    1. 1110011001.
    2. 0100111111.
    3. 0111001110.

4. 0101010001.
5. 1010101111.

8. Подходы, которые применяются для обеспечения безопасной передачи данных по сети на двух нижних уровнях модели сетевого взаимодействия:
    1. административная защита на маршрутизаторах.
    2. фильтрация трафика между внутренней сетью и внешней коммуникационной средой.
    3. защита при помощи межсетевых экранов.
    4. шифрование соединения.
    5. выборочное или полное шифрование трафика.
9. Вредосносные программы, требующие наличия программы-носителя:
    1. бактерии.
    2. логические бомбы.
    3. троянские кони.
    4. черви.
    5. вирусы.
10. Брандмауэр:
    1. может защитить от внутренних угроз безопасности.
    2. не может защитить от внутренних угроз безопасности, например со стороны сотрудника, вступившего в сговор с внешним нарушителем.
    3. не может фильтровать электронную почту, отсеивая «спам».
    4. может разрешить доступ извне только к определенной части информации, находящейся на локальном Web-сервере.
    5. не может защитить от угрозы передачи инфицированных вирусами программ или файлов.

9.1.3. Примерный перечень вариантов (заданий) контрольных работ

1. Целостность:
    1. свойство информации, выражающееся в строгой принадлежности объекту, который является ее источником, либо тому объекту, от которого эта информация принята.
    2. способность информации быть доступной для конечного пользователя в соответствии с его временными потребностями.
    3. свойство информации или программного обеспечения сохранять свою структуру и/или содержание в процессе передачи и/или хранения.
    4. способность совершать некоторые действия в информационной системе незаметно для других объектов.
    5. свойство информации быть доступной ограниченному кругу пользователей информационной системы, в которой циркулирует данная информация.
2. Достоверность:
    1. свойство информации, выражающееся в строгой принадлежности объекту, который является ее источником, либо тому объекту, от которого эта информация принята.
    2. способность информации быть доступной для конечного пользователя в соответствии с его временными потребностями.
    3. свойство информации или программного обеспечения сохранять свою структуру и/или содержание в процессе передачи и/или хранения.
    4. способность совершать некоторые действия в информационной системе незаметно для других объектов.
    5. свойство информации быть доступной ограниченному кругу пользователей информационной системы, в которой циркулирует данная информация.
3. Полиграмный подстановочный шифр:
    1. один символ открытого текста отображается на один символ шифротекста.
    2. один символ открытого текста отображает на несколько символов шифротекста.
    3. блоки символов шифрует по группам.
    4. применяет псевдослучайный ключ.
    5. применяет открытый ключ.

4. В полиалфавитном подстановочном шифре:
    1. применяется псевдослучайный ключ.
    2. применяется имитовставка.
    3. применяется открытый ключ.
    4. длина ключа равна длине сообщения.
    5. применяются несколько простых подстановочных шифров.
5. Безопасность симметричного алгоритма определяется:
    1. ключом.
    2. функцией шифрования.
    3. функцией дешифрования.
    4. применением двух ключей.
    5. применением разных ключей для шифрования и дешифрования.
6. Расстояние уникальности измеряет:
    1. количество криптотекста нужного для криптоанализа.
    2. минимальное количество криптотекста, необходимое для единственности результата криптоанализа.
    3. сумму энтропии киптосистемы и энтропии ключа шифрования.
    4. избыточность криптосиситемы.
    5. точную длину шифротекста.
7. Основные отличия блочного шифра от поточного:
    1. за один прием обрабатывается блок открытого текста.
    2. при шифровании необходимо постоянно помнить, какое место в строке в данный момент обрабатывается.
    3. более общий – легко трансформируется в поточный.
    4. использует более математизированную структуру.
    5. более быстрый, чем поточный.
8. Защиту информации на физическом и канальном уровне обеспечивают такие устройства как:
    1. шифрующие модемы.
    2. специализированные канальные адаптеры.
    3. криптосерверы.
    4. шифрующие маршрутизаторы.
    5. proxy-серверы.
9. Какие могут быть заданы действия или события, по наступлению которых активизируется лазейка:
    1. введение с клавиатуры специальной последовательности.
    2. введение определенного идентификатора пользователя.
    3. наступление определенного дня недели.
    4. последовательность каких-то маловероятных событий.
    5. наступление определенной даты.
10. Брандмауэр представляет собой:
    1. единственную точку входа, в которой предотвращается санкционированный доступ внешних пользователей к защищаемой сети, запрещается потенциально уязвимым службам доступ к внутренней сети извне или отправка данных изнутри во внешний мир, также обеспечивается защита от различных атак вторжения с помощью изменения маршрута или указания ложных IP-адресов.
    2. одну из точек входа, в которой предотвращается несанкционированный доступ внешних пользователей к защищаемой сети, запрещается потенциально уязвимым службам доступ к внутренней сети извне или отправка данных изнутри во внешний мир, также обеспечивается защита от различных атак вторжения с помощью изменения маршрута или указания ложных IP-адресов.
    3. единственную точку входа, в которой возможен несанкционированный доступ внешних пользователей к защищаемой сети, запрещается потенциально уязвимым службам доступ к внутренней сети извне или отправка данных изнутри во внешний мир, также обеспечивается защита от различных атак вторжения с помощью изменения маршрута или указания ложных IP-адресов.
    4. единственную точку входа, в которой предотвращается несанкционированный

доступ внешних пользователей к защищаемой сети, однако не запрещается потенциально уязвимым службам доступ к внутренней сети извне или отправка данных изнутри во внешний мир, также обеспечивается защита от различных атак вторжения с помощью изменения маршрута или указания ложных IP-адресов.

5. единственную точку входа, в которой предотвращается несанкционированный доступ внешних пользователей к защищаемой сети, запрещается потенциально уязвимым службам доступ к внутренней сети извне или отправка данных изнутри во внешний мир, также обеспечивается защита от различных атак вторжения с помощью изменения маршрута или указания ложных IP-адресов.

9.1.4. Темы лабораторных работ

1. Администрирование учетных записей пользователей.
2. Управление параметрами операционной системы.
3. Дискреционный механизм разграничения доступа.
4. Политика ограниченного использования программ.

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 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 9.4.

Таблица 9.4 – 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, 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.

ЛИСТ СОГЛАСОВАНИЯ

Рассмотрена и одобрена на заседании кафедры АСУ
протокол № 11 от «23» 11 2023 г.

СОГЛАСОВАНО:

Должность	Инициалы, фамилия	Подпись
Заведующий выпускающей каф. АСУ	В.В. Романенко	Согласовано, c3e2018f-3231-48c3-b093-89b6f5342191
Заведующий обеспечивающей каф. АСУ	В.В. Романенко	Согласовано, c3e2018f-3231-48c3-b093-89b6f5342191
Начальник учебного управления	И.А. Лариошина	Согласовано, c3195437-a02f-4972-a7c6-ab6ee1f21e73

ЭКСПЕРТЫ:

Доцент, каф. АСУ	А.И. Исакова	Согласовано, 79bf1038-9d22-4279-a1e8-7806307b7f82
Доцент, каф. АСУ	А.И. Исакова	Согласовано, 79bf1038-9d22-4279-a1e8-7806307b7f82

РАЗРАБОТАНО:

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