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 учебной работе

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

ЗАЩИТА ИНФОРМАЦИИ

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки / специальность: **09.03.02 Информационные системы и технологии**
Направленность (профиль) / специализация: **Аналитические информационные системы**
Форма обучения: **очная**
Факультет: **Факультет вычислительных систем (ФВС)**
Кафедра: **Кафедра экономической математики, информатики и статистики (ЭМИС)**
Курс: **4**
Семестр: **7**
Учебный план набора 2021 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	7 семестр	Всего	Единицы
Лекционные занятия	18	18	часов
Лабораторные занятия	36	36	часов
Самостоятельная работа	54	54	часов
Подготовка и сдача экзамена	36	36	часов
Общая трудоемкость (включая промежуточную аттестацию)	144	144	часов
	4	4	з.е.

Формы промежуточной аттестация	Семестр
Экзамен	7

Томск

1. Общие положения

1.1. Цели дисциплины

1. Дать представление о сущности и значении информации в развитии современного информационного общества, о необходимости соблюдения основных требований к информационной безопасности.

1.2. Задачи дисциплины

1. Дать будущим специалистам необходимые для их работы теоретические знания о современных средствах, методах и технологиях обеспечения информационной безопасности.
2. Сформировать у студентов практические навыки организации работ по обеспечению информационной безопасности на предприятиях.

2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).
Часть блока дисциплин: Обязательная часть.
Модуль дисциплин: Модуль направления подготовки (special hard skills - SHS).
Индекс дисциплины: Б1.О.03.09.
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-2. Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности	ОПК-2.1. Знает основы информационных технологий и программирования и основные компоненты программных средств, а также их назначение и состав	Выделяет основные компоненты информационных технологий и программных средств, знает их назначение и состав
	ОПК-2.2. Умеет выбирать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности, а также обосновывать их выбор	Умеет классифицировать информационные технологии и программные средства (в том числе и отечественного производства) для обоснования выбора при решении профессиональных задач
	ОПК-2.3. Владеет навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности	Обосновывает выбор информационных технологий и средств для решения задач профессиональной деятельности

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	Выделяет критерии поиска, анализа и синтеза информации для решения стандартных профессиональных задач
	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	Владеет современными информационно-коммуникационными технологиями
	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	Выделяет и применяет требования информационной безопасности при решении стандартных профессиональных задач
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
Контактная аудиторная работа обучающихся с преподавателем, всего	54	54
Лекционные занятия	18	18
Лабораторные занятия	36	36
Самостоятельная работа обучающихся, в т.ч. контактная внеаудиторная работа обучающихся с преподавателем, всего	54	54
Подготовка к тестированию	30	30
Подготовка к лабораторной работе, написание отчета	24	24
Подготовка и сдача экзамена	36	36
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	Лек. зан., ч	Лаб. раб.	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
7 семестр					
1 Введение	2	-	4	6	ОПК-2, ОПК-3
2 Проблемы и методы защиты информации	4	-	6	10	ОПК-2, ОПК-3
3 Математические и методологические средства защиты информации	4	10	12	26	ОПК-2, ОПК-3
4 Криптографические алгоритмы обеспечения информационной безопасности	4	16	14	34	ОПК-2, ОПК-3
5 Компьютерные средства реализации защиты в информационных системах	4	10	18	32	ОПК-2, ОПК-3
Итого за семестр	18	36	54	108	
Итого	18	36	54	108	

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	Цель и задачи дисциплины, ее роль и место в общей системе подготовки специалиста. Защита информации и информационная безопасность как важный фактор политической и экономической составляющих национальной безопасности. Программа информационной безопасности России и пути ее реализации.	2	ОПК-2, ОПК-3
	Итого	2	
2 Проблемы и методы защиты информации	Информационная безопасность. Проблемы защиты информации в компьютерных системах. Защита информации при реализации информационных процессов ввода, вывода, передачи, обработки, накопления и хранения информации. Организационное обеспечение информационной безопасности.	4	ОПК-2, ОПК-3
	Итого	4	

3 Математические и методологические средства защиты информации	Криптографическая терминология. Сведения из теории информации и теории чисел. Алгоритмы и ключи. Симметричные алгоритмы. Алгоритмы с открытым ключом. Подстановочные и перестановочные шифры. Одноразовые блокноты. Однонаправленные хэш-функции. Передача информации с использованием криптографии с открытым ключом. Основные протоколы передачи информации.	4	ОПК-2, ОПК-3
	Итого	4	
4 Криптографические алгоритмы обеспечения информационной безопасности	Алгоритм симметричного шифрования данных DES. Алгоритм криптографического преобразования. Асимметричный алгоритм шифрования данных RSA. Комплекс криптографических алгоритмов PGP. Защита информации от несанкционированного доступа.	4	ОПК-2, ОПК-3
	Итого	4	
5 Компьютерные средства реализации защиты в информационных системах	Физический, сетевой, транспортный и прикладной уровни защиты информации. Обзор стандартов в области защиты информации. Методы и средства защиты локальной рабочей станции. Защита в локальных сетях. Защита информации при межсетевом взаимодействии. Типы вирусов и средства антивирусной защиты. Обеспечение информационной безопасности в корпоративных сетях.	4	ОПК-2, ОПК-3
	Итого	4	
Итого за семестр		18	
Итого		18	

5.3. Практические занятия (семинары)

Не предусмотрено учебным планом

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			
3 Математические и методологические средства защиты информации	Шифрование и дешифрирование информации. Реализация методов защиты информации. Метод Полибия.	10	ОПК-2, ОПК-3
	Итого	10	

4 Криптографические алгоритмы обеспечения информационной безопасности	Разработка программы шифрования на основе метода замены. Разработка программы шифрования на основе метода умножения матриц.	16	ОПК-2, ОПК-3
	Итого	16	
5 Компьютерные средства реализации защиты в информационных системах	Разработка программной реализации асимметричного алгоритма шифрования данных RSA. Комплекс криптоалгоритмов PGP.	10	ОПК-2, ОПК-3
	Итого	10	
Итого за семестр		36	
Итого		36	

5.5. Курсовой проект / курсовая работа

Не предусмотрено учебным планом

5.6. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 5.6.

Таблица 5.6 – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов (тем) дисциплины	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
7 семестр				
1 Введение	Подготовка к тестированию	4	ОПК-2, ОПК-3	Тестирование
	Итого	4		
2 Проблемы и методы защиты информации	Подготовка к тестированию	6	ОПК-2, ОПК-3	Тестирование
	Итого	6		
3 Математические и методологические средства защиты информации	Подготовка к тестированию	6	ОПК-2, ОПК-3	Тестирование
	Подготовка к лабораторной работе, написание отчета	6	ОПК-2, ОПК-3	Лабораторная работа
	Итого	12		
4 Криптографические алгоритмы обеспечения информационной безопасности	Подготовка к тестированию	6	ОПК-2, ОПК-3	Тестирование
	Подготовка к лабораторной работе, написание отчета	8	ОПК-2, ОПК-3	Лабораторная работа
	Итого	14		

5 Компьютерные средства реализации защиты в информационных системах	Подготовка к тестированию	8	ОПК-2, ОПК-3	Тестирование
	Подготовка к лабораторной работе, написание отчета	10	ОПК-2, ОПК-3	Лабораторная работа
	Итого	18		
Итого за семестр		54		
	Подготовка и сдача экзамена	36		Экзамен
Итого		90		

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

Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной деятельности представлено в таблице 5.7.

Таблица 5.7 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Формируемые компетенции	Виды учебной деятельности			Формы контроля
	Лек. зан.	Лаб. раб.	Сам. раб.	
ОПК-2	+	+	+	Лабораторная работа, Тестирование, Экзамен
ОПК-3	+	+	+	Лабораторная работа, Тестирование, Экзамен

6. Рейтинговая система для оценки успеваемости обучающихся

6.1. Балльные оценки для форм контроля

Балльные оценки для форм контроля представлены в таблице 6.1.

Таблица 6.1 – Балльные оценки

Формы контроля	Максимальный балл на 1-ую КТ с начала семестра	Максимальный балл за период между 1КТ и 2КТ	Максимальный балл за период между 2КТ и на конец семестра	Всего за семестр
7 семестр				
Лабораторная работа	15	10	15	40
Тестирование	10	10	10	30
Экзамен				30
Итого максимум за период	25	20	25	100
Нарастающим итогом	25	45	70	100

6.2. Пересчет баллов в оценки за текущий контроль

Пересчет баллов в оценки за текущий контроль представлен в таблице 6.2.

Таблица 6.2 – Пересчет баллов в оценки за текущий контроль

Баллы на дату текущего контроля	Оценка
≥ 90% от максимальной суммы баллов на дату ТК	5
От 70% до 89% от максимальной суммы баллов на дату ТК	4
От 60% до 69% от максимальной суммы баллов на дату ТК	3
< 60% от максимальной суммы баллов на дату ТК	2

6.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 6.3.

Таблица 6.3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка	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)

7. Учебно-методическое и информационное обеспечение дисциплины

7.1. Основная литература

1. Гультяева, Т. А. Основы защиты информации : учебное пособие / Т. А. Гультяева. — Новосибирск : НГТУ, 2018. — 83 с. — ISBN 978-5-7782-3641-7. — Текст : электронный // Лань : электронно-библиотечная система. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/118234 .

2. Груздева, Л. М. Защита информации : учебное пособие / Л. М. Груздева. — Москва : РУТ (МИИТ), 2019. — 144 с. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/188703.

7.2. Дополнительная литература

1. Защита прав интеллектуальной собственности: Учебное пособие / А. Н. Сычев - 2014. 240 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/4967.

2. Исследование методов кодирования и шифрования : учебное пособие / А. П. Алексеев, М. И. Макаров, О. В. Сирант, С. С. Яковлева ; под редакцией А. П. Алексеева. — Самара : ПГУТИ, 2018. — 102 с. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/182252.

7.3. Учебно-методические пособия

7.3.1. Обязательные учебно-методические пособия

1. Защита информации: Методические указания к выполнению самостоятельных работ / В. Г. Спицын - 2012. 78 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/2261.

2. Защита информации: Методические указания к выполнению лабораторных работ / В. Г. Спицын - 2012. 17 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/1822.

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;

– 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

Класс ГПО: учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа, помещение для курсового проектирования (выполнения курсовых работ), помещение для проведения групповых и индивидуальных консультаций, помещение для проведения текущего контроля и промежуточной аттестации, помещение для самостоятельной работы; 634034, Томская область, г. Томск, Вершинина улица, д. 74, 425 ауд.

Описание имеющегося оборудования:
- Плазменный телевизор;
- Магнитно-маркерная доска;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:
- 7-Zip;
- Google Chrome;
- Microsoft Office 95;
- Microsoft Visual Studio 2012;
- Microsoft Windows 7 Pro;
- OpenOffice;

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, 201 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.

8.4. 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	ОПК-2, ОПК-3	Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
2 Проблемы и методы защиты информации	ОПК-2, ОПК-3	Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
3 Математические и методологические средства защиты информации	ОПК-2, ОПК-3	Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
4 Криптографические алгоритмы обеспечения информационной безопасности	ОПК-2, ОПК-3	Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов

5 Компьютерные средства реализации защиты в информационных системах	ОПК-2, ОПК-3	Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов

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:
   не может различаться
   может различаться
   должно быть равно сумме знаков открытого текста и ключа
   должно быть равно разности знаков открытого текста и ключа
2. Стойкость современных криптосистем основывается на:
   секретности долговременных элементов криптозащиты
   применении стеганографических алгоритмов
   секретности алгоритма шифрования
   секретности информации сравнительно малого размера, называемой ключом
3. Идентификация законных пользователей заключается в:
   сравнении пароля, вводимого пользователем, с паролем, хранящимся в явном виде в ЭВМ
   сравнении пароля, вводимого пользователем, с образом пароля, хранящимся в ЭВМ
   сравнении образа пароля, вводимого пользователем, с образом пароля, хранящегося в явном виде в ЭВМ
   сравнении пароля, вводимого пользователем, с открытым ключом, хранящимся в ЭВМ
4. Подстановочным шифром называется шифр, в котором:
   используется матрица чисел размерностью 5x5
   используется открытый ключ
   используется фрагмент текста и открытый ключ
   каждый символ открытого текста в шифротексте заменяется другим символом
5. В шифре Цезаря каждый символ открытого текста:
   заменяется символом, находящимся двумя символами правее по модулю 26
   заменяется символом, находящимся семью символами правее по модулю 26
   заменяется символом, находящимся тремя символами правее по модулю 26
   заменяется символом, находящимся пятью символами правее по модулю 26
6. Для осмысленного текста, написанного на английском языке индекс совпадений равен:
   0.521
   0.332
   0.024
   0.065
7. Безопасность симметричного алгоритма определяется:
   применением разных ключей для шифрования и дешифрования
   ключом
   применением двух ключей
   литературными данными
8. Асимметричный шифр отличается от симметричного тем, что:
   ключ шифрования отличается от ключа дешифрования
   ключ дешифрирования может быть рассчитан по ключу шифрования
   ключ шифрования совпадает с ключом дешифрования
   используются несколько ключей для шифрования
9. Смешанные криптосистемы основаны на совместном применении:
   симметричных алгоритмов и алгоритмов с открытыми ключами

нескольких двухключевых алгоритмов
нескольких одноключевых алгоритмов
потоковых и блочных алгоритмов

10. В шифре DES применяется количество подключей n, причем каждый из подключей имеет размер m бит:
n=64, m=256
n=32, m=64
n=8, m=32
n=16, m=48

9.1.2. Перечень экзаменационных вопросов

1. Защита информации и информационная безопасность как важный фактор политической и экономической составляющих национальной безопасности.
2. Программа информационной безопасности России и пути ее реализации.
3. Проблемы защиты информации в компьютерных системах.
4. Защита информации при реализации информационных процессов ввода, вывода, передачи, обработки, накопления и хранения информации.
5. Организационное обеспечение информационной безопасности.
6. Криптографическая терминология.
7. Алгоритмы и ключи.
8. Симметричные алгоритмы.
9. Алгоритмы с открытым ключом.
10. Подстановочные и перестановочные шифры.
11. Одноразовые блокноты.
12. Однонаправленные хэш-функции.
13. Передача информации с использованием криптографии с открытым ключом.
14. Алгоритм симметричного шифрования данных DES.
15. Асимметричный алгоритм шифрования данных RSA.
16. Комплекс криптографических алгоритмов PGP.
17. Защита информации от несанкционированного доступа.
18. Физический, сетевой, транспортный и прикладной уровни защиты информации.
19. Обзор стандартов в области защиты информации.
20. Методы и средства защиты локальной рабочей станции.
21. Защита в локальных сетях.
22. Защита информации при межсетевом взаимодействии.
23. Типы вирусов и средства антивирусной защиты.
24. Обеспечение информационной безопасности в корпоративных сетях.

9.1.3. Темы лабораторных работ

1. Шифрование и дешифрирование информации. Реализация методов защиты информации. Метод Полибия.
2. Разработка программы шифрования на основе метода замены. Разработка программы шифрования на основе метода умножения матриц.
3. Разработка программной реализации асимметричного алгоритма шифрования данных RSA. Комплекс криптоалгоритмов PGP.

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
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 ЭМИС
протокол № 4 от «14» 12 2020 г.

СОГЛАСОВАНО:

Должность	Инициалы, фамилия	Подпись
Заведующий выпускающей каф. ЭМИС	И.Г. Боровской	Согласовано, 806d2ff7-778b-4ed6-a3d7-87623a208b8c
Заведующий обеспечивающей каф. ЭМИС	И.Г. Боровской	Согласовано, 806d2ff7-778b-4ed6-a3d7-87623a208b8c
Начальник учебного управления	Е.В. Саврук	Согласовано, fa63922b-1fce-4a6a-845d-9ce7670b004c

ЭКСПЕРТЫ:

Старший преподаватель, каф. ЭМИС	И.Г. Афанасьева	Согласовано, 14d2ad0b-0b75-401e-9d97-39fca5825785
Доцент, каф. ЭМИС	Е.А. Шельмина	Согласовано, 54cb71d7-43bf-4e94-938e-094b7e6d003d

РАЗРАБОТАНО:

Доцент, каф. ЭМИС	Е.А. Шельмина	Разработано, 54cb71d7-43bf-4e94-938e-094b7e6d003d