МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
И.о. проректора по УРиМД
_____Нариманова Г.Н.
«05» _____03_____ 2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки / специальность: **11.03.02 Инфокоммуникационные технологии и системы связи**
Направленность (профиль) / специализация: **Интеллектуальные системы связи**
Форма обучения: **очная**
Факультет: **Институт радиоэлектронной техники (ИРЭТ)**
Кафедра: **институт радиоэлектронной техники (ИРЭТ)**
Курс: **3**
Семестр: **6**
Учебный план набора 2025 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	6 семестр	Всего	Единицы
Лекционные занятия	12	12	часов
Лабораторные занятия	24	24	часов
Самостоятельная работа	36	36	часов
Общая трудоемкость (включая промежуточную аттестацию)	72	72	часов
	2	2	з.е.

Формы промежуточной аттестации	Семестр
Зачет	6

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Нариманова Г.Н.
Должность: И.о. проректора по УРиМД
Дата подписания: 05.03.2025
Уникальный программный ключ:
eb4e14e0-de8d-48f7-bf05-ceacb167edfe

Томск

Согласована на портале № 82945

1. Общие положения

1.1. Цели дисциплины

1. Изучение комплекса проблем информационной безопасности предприятий и организаций различных типов и направлений деятельности построения, функционирования и совершенствования совокупности правовых, организационных, технических и технологических процессов, обеспечивающих информационную безопасность и формирующих структуру системы защиты ценной и конфиденциальной информации в сфере охраны интеллектуальной собственности и сохранности информационных ресурсов.

1.2. Задачи дисциплины

1. Ознакомление студентов с теоретическими основами, основными понятиями и принципами обеспечения информационной безопасности.
2. Обучение студентов работе с основными средствами защиты.

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.03.08.
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 № 82945

ОПК-3. Способен применять методы поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности	ОПК-3.1. Знает принципы поиска, хранения, обработки, анализа и представления информации, а также методы и средства обеспечения информационной безопасности	Знает методы и средства защиты информационной безопасности направления и методы ведения аналитической работы по выявлению угроз технические процедуры по действиям в нештатной ситуации; методологии оценки рисков и угроз информационной безопасности.
	ОПК-3.2. Умеет работать с источниками информации и базами данных, а также решать задачи обработки данных с помощью современных средств автоматизации	Умеет оценивать и выбирать необходимые средства защиты осуществлять мониторинг состояния информационной безопасности объекта; обеспечивать противодействие атакам на информационную систему; выполнять (контролировать выполнение) требований инструкции по обеспечению информационной безопасности.
	ОПК-3.3. Владеет практическими навыками поиска, хранения, обработки, анализа и представления в требуемом формате необходимой информации и обеспечения информационной безопасности при решении задач в области профессиональной деятельности	Владеет навыками работы с программными и аппаратными средствами обеспечивающими защиту информации в компьютерных системах.
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 2 зачетных единиц, 72 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
		6 семестр
Контактная аудиторная работа обучающихся с преподавателем, всего	36	36
Лекционные занятия	12	12
Лабораторные занятия	24	24
Самостоятельная работа обучающихся, в т.ч. контактная внеаудиторная работа обучающихся с преподавателем, всего	36	36
Подготовка к тестированию	14	14
Подготовка к зачету	14	14
Подготовка к лабораторной работе, написание отчета	8	8
Общая трудоемкость (в часах)	72	72
Общая трудоемкость (в з.е.)	2	2

Согласована на портале № 82945

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
6 семестр					
1 Базовые понятия в сфере обеспечения информационной безопасности	2	-	4	6	ОПК-3
2 Комплексный подход к обеспечению информационной безопасности	2	-	4	6	ОПК-3
3 Организационно-правовое обеспечение, стандартизация, сертификация и лицензирование в области защиты информации	2	-	2	4	ОПК-3
4 Методы оценки рисков и угроз информационной безопасности	1	-	2	3	ОПК-3
5 Программно-аппаратные, технические и криптографические средства защиты информации	1	24	10	35	ОПК-3
6 Основные принципы, направления и требования обеспечения информационной безопасности организации	1	-	4	5	ОПК-3
7 Концепция и политика информационной безопасности	1	-	4	5	ОПК-3
8 Реализации стратегии обеспечения информационной безопасности	1	-	2	3	ОПК-3
9 Менеджмент информационной безопасности	1	-	4	5	ОПК-3
Итого за семестр	12	24	36	72	
Итого	12	24	36	72	

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
6 семестр			
1 Базовые понятия в сфере обеспечения информационной безопасности	Информация. Конфиденциальность. Целостность. Доступность. Свойства информации. Угроза. Нарушитель	2	ОПК-3
	Итого	2	
2 Комплексный подход к обеспечению информационной безопасности	Структура системы защиты информации.	2	ОПК-3
	Итого	2	

Согласована на портале № 82945

3 Организационно-правовое обеспечение, стандартизация, сертификация и лицензирование в области защиты информации	Основные нормативно правовые акты по защите информации. Стандартизация. Сертификация. Лицензирование	2	ОПК-3
	Итого	2	
4 Методы оценки рисков и угроз информационной безопасности	Оценка рисков. Информационные измерения. Нечеткая кластеризация. Идентификация и анализ рисков.	1	ОПК-3
	Итого	1	
5 Программно-аппаратные, технические и криптографические средства защиты информации	Управление доступом. Разграничение уровней доступа. Дискретное распределение доступа. Мандатное распределение доступа.	1	ОПК-3
	Итого	1	
6 Основные принципы, направления и требования обеспечения информационной безопасности организации	Определение организационных требований защиты ИТ.	1	ОПК-3
	Итого	1	
7 Концепция и политика информационной безопасности	Политика безопасности.	1	ОПК-3
	Итого	1	
8 Реализации стратегии обеспечения информационной безопасности	Определение организационных целей и стратегий защиты ИТ. Идентификация и анализ угроз активам ИТ в пределах организации. Определение соответствующих защитных мер.	1	ОПК-3
	Итого	1	
9 Менеджмент информационной безопасности	Контроль выполнения и функционирования защитных мер. Разработка и реализация программы осведомленности о защите. Обнаружение инцидентов и реагирование на них.	1	ОПК-3
	Итого	1	
	Итого за семестр	12	
	Итого	12	

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

Согласована на портале № 82945

Названия разделов (тем) дисциплины	Наименование лабораторных работ	Трудоемкость, ч	Формируемые компетенции
6 семестр			
5 Программно-аппаратные, технические и криптографические средства защиты информации	Методы донаучной криптографии	8	ОПК-3
	Электронная цифровая подпись	8	ОПК-3
	Практическое применение криптографии с открытым ключом	8	ОПК-3
	Итого	24	
Итого за семестр		24	
Итого		24	

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
6 семестр				
1 Базовые понятия в сфере обеспечения информационной безопасности	Подготовка к тестированию	2	ОПК-3	Тестирование
	Подготовка к зачету	2	ОПК-3	Зачёт
	Итого	4		
2 Комплексный подход к обеспечению информационной безопасности	Подготовка к тестированию	2	ОПК-3	Тестирование
	Подготовка к зачету	2	ОПК-3	Зачёт
	Итого	4		
3 Организационно-правовое обеспечение, стандартизация, сертификация и лицензирование в области защиты информации	Подготовка к тестированию	1	ОПК-3	Тестирование
	Подготовка к зачету	1	ОПК-3	Зачёт
	Итого	2		
4 Методы оценки рисков и угроз информационной безопасности	Подготовка к тестированию	1	ОПК-3	Тестирование
	Подготовка к зачету	1	ОПК-3	Зачёт
	Итого	2		

Согласована на портале № 82945

5 Программно-аппаратные, технические и криптографические средства защиты информации	Подготовка к тестированию	1	ОПК-3	Тестирование
	Подготовка к зачету	1	ОПК-3	Зачёт
	Подготовка к лабораторной работе, написание отчета	8	ОПК-3	Лабораторная работа
	Итого	10		
6 Основные принципы, направления и требования обеспечения информационной безопасности организации	Подготовка к тестированию	2	ОПК-3	Тестирование
	Подготовка к зачету	2	ОПК-3	Зачёт
	Итого	4		
7 Концепция и политика информационной безопасности	Подготовка к тестированию	2	ОПК-3	Тестирование
	Подготовка к зачету	2	ОПК-3	Зачёт
	Итого	4		
8 Реализации стратегии обеспечения информационной безопасности	Подготовка к тестированию	1	ОПК-3	Тестирование
	Подготовка к зачету	1	ОПК-3	Зачёт
	Итого	2		
9 Менеджмент информационной безопасности	Подготовка к тестированию	2	ОПК-3	Тестирование
	Подготовка к зачету	2	ОПК-3	Зачёт
	Итого	4		
Итого за семестр		36		
Итого		36		

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

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий 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-3	+	+	+	Зачёт, Лабораторная работа, Тестирование

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

Согласована на портале № 82945

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
6 семестр				
Зачёт	0	0	30	30
Лабораторная работа	15	15	10	40
Тестирование	10	10	10	30
Итого максимум за период	25	25	50	100
Нарастающим итогом	25	50	100	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. 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.

2. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 161 с. [Электронный ресурс]: — Режим доступа: https://urait.ru/bcode/537247.

7.2. Дополнительная литература

1. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2022. — 104 с. [Электронный ресурс]: — Режим доступа: https://urait.ru/bcode/497002.

Согласована на портале № 82945

2. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2024. — 309 с. [Электронный ресурс]: — Режим доступа: https://urait.ru/bcode/537000.

7.3. Учебно-методические пособия

7.3.1. Обязательные учебно-методические пособия

1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: Методические указания к лабораторным работам, практическим занятиям и организации самостоятельной работы для студентов технических направлений подготовки всех форм обучения / А. Н. Горитов - 2022. 15 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/10838.

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

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

Аудитория моделирования, проектирования и эксплуатации информационных и аналитических систем: учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа; 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 407 ауд.

Описание имеющегося оборудования:
- Интерактивная сенсорная панель 75";
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:
- Kaspersky endpoint security;
- KasperskySecurityCenter;
- Microsoft Windows 10;
- VirtualBox;

Согласована на портале № 82945

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, 101 ауд.;
- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 107 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 130 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 Базовые понятия в сфере обеспечения информационной безопасности	ОПК-3	Зачёт	Перечень вопросов для зачета
		Тестирование	Примерный перечень тестовых заданий

Согласована на портале № 82945

2 Комплексный подход к обеспечению информационной безопасности	ОПК-3	Зачёт	Перечень вопросов для зачета
		Тестирование	Примерный перечень тестовых заданий
3 Организационно-правовое обеспечение, стандартизация, сертификация и лицензирование в области защиты информации	ОПК-3	Зачёт	Перечень вопросов для зачета
		Тестирование	Примерный перечень тестовых заданий
4 Методы оценки рисков и угроз информационной безопасности	ОПК-3	Зачёт	Перечень вопросов для зачета
		Тестирование	Примерный перечень тестовых заданий
5 Программно-аппаратные, технические и криптографические средства защиты информации	ОПК-3	Зачёт	Перечень вопросов для зачета
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
6 Основные принципы, направления и требования обеспечения информационной безопасности организации	ОПК-3	Зачёт	Перечень вопросов для зачета
		Тестирование	Примерный перечень тестовых заданий
7 Концепция и политика информационной безопасности	ОПК-3	Зачёт	Перечень вопросов для зачета
		Тестирование	Примерный перечень тестовых заданий
8 Реализации стратегии обеспечения информационной безопасности	ОПК-3	Зачёт	Перечень вопросов для зачета
		Тестирование	Примерный перечень тестовых заданий
9 Менеджмент информационной безопасности	ОПК-3	Зачёт	Перечень вопросов для зачета
		Тестирование	Примерный перечень тестовых заданий

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

Согласована на портале № 82945

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. Какая из нижеперечисленных задач, изложенных в Доктрине информационной безопасности Российской Федерации, не относится к задачам государственных органов в рамках деятельности по обеспечению информационной безопасности:
   a) обеспечение защиты прав и законных интересов граждан и организаций в информационной сфере;
   b) оценка состояния информационной безопасности, прогнозирование и обнаружение информационных угроз, определение приоритетных направлений их предотвращения и ликвидации последствий их проявления;
   c) планирование и разработка мер по проведению киберразведовательных операций;

Согласована на портале № 82945

d) организация деятельности и координация взаимодействия сил обеспечения информационной безопасности, совершенствование их правового, организационного, оперативно-разыскного, разведывательного, контрразведывательного, научно-технического, информационно-аналитического, кадрового и экономического обеспечения.

2. В стандарте США "Критерии оценки гарантировано защищенных вычислительных систем в интересах министерства обороны США" в зависимости от конкретных значений, которым отвечают автоматизированные системы, они разделены на…
   a) 5 классов;
   b) 4 группы;
   c) 3 множества;
   d) 2 подгруппы.
3. Что из нижеперечисленного не относится к перечню сведений конфиденциального характера, утвержденного Президентом Российской Федерации?
   a) Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);
   b) Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;
   c) Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).
4. Стандарт США «Критерии оценки гарантировано защищенных вычислительных систем в интересах министерства обороны США» называют …
   a) «Желтой книгой»;
   b) «Оранжевым документом»;
   c) «Оранжевой книгой»;
   d) «Красным списком».
5. Модель угроз безопасности информации не включает в себя:
   a) Описание информационной системы и ее структурно-функциональных характеристик;
   b) Описание угроз безопасности информации;
   c) Описание возможностей нарушителей (модель нарушителя), возможных уязвимостей информационной системы;
   d) Стадии (этапы работ) создания системы защиты информационной системы.
6. При макетировании и тестировании системы защиты информации информационной системы в том числе осуществляются:
   a) Проверка работоспособности и совместимости выбранных средств защиты информации с информационными технологиями и техническими средствами;
   b) Установка средств мониторинга сетевой инфраструктуры;
   c) Разработка документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации;
   d) Внедрение документов, регламентирующих организационные меры по защите информации.
7. Методический документ ФСТЭК России «Методика определения безопасности информации в информационных системах» применяется совместно с:
   a) Базой данных уязвимостей, разработанной Федеральной службой безопасности Российской Федерации;
   b) Банком данных угроз безопасности информации, сформированным ФСТЭК России (ubi.fstec.ru);
   c) Общедоступной базой данных компьютерных угроз;
   d) Перечнем сведений конфиденциального характера.
8. Анализ уязвимостей информационной системы проводится в целях:
   a) Оценки возможности преодоления нарушителем системы защиты информации

Согласована на портале № 82945

информационной системы и предотвращения реализации угроз безопасности информации;
b) Оценки эффективности использования политик разграничения доступа;
c) Оптимизации производительности программно-аппаратных средств защиты информации;
d) Сегментации информационной системы.

9. Системный процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности компании в соответствии с определёнными критериями и показателями безопасности называется:
a) Аттестация;
b) Аудит;
c) Сертификация;
d) Пентест.
10. Что из нижеперечисленного не относится к международным методикам проведения тестирования на проникновение, ориентированных на моделирование атак, направленных на сетевую инфраструктуру организации:
a) Trusted Computer System Evaluation Criteria;
b) PCI DSS;
c) NIST SP800-115;
d) Open Source Security Testing Methodology Manual.
11. Абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа называется:
a) Характеристика нарушителя;
b) Модель нарушителя;
c) Сценарий нарушителя;
d) Модель источников угроз.
12. Какое из нижеперечисленных направлений не относится к аттестации объектов информатизации по требованиям безопасности информации:
a) Аттестация автоматизированных систем, средств связи, обработки и передачи информации;
b) Аттестация помещений, предназначенных для ведения конфиденциальных переговоров;
c) Аттестация рабочих мест с целью оценки условий труда;
d) Аттестация технических средств, установленных в выделенных помещениях и защищаемых помещениях.
13. Стратегия (метод) тестирования функционального поведения объекта (программы, системы) с точки зрения внешнего мира, при котором не используется знание о внутреннем устройстве тестируемого объекта
a) Тестировение черного ящика;
b) Тестирование белого ящика;
c) Тестирование красного ящика;
d) Тестирование неизвестного ящика.
14. Методика тестирования на проникновение называется:
a) Аудит;
b) Пентест;
c) Honeypot;
d) Metasploit
15. Что из нижеперечисленного не относится к этапу анализа рисков информационной безопасности:
a) Построение модели нарушителя;
b) Идентификация ресурсов;
c) Идентификация бизнес-требований и требований законодательства, применимых к идентифицированным ресурсам; d) Оценивание идентифицированных ресурсов с учетом выявленных бизнес требований и требований законодательства, а также последствий нарушения их конфиденциальности, целостности и доступности.
16. Какая угроза безопасности информации является преднамеренной ?
a) Ошибки персонала;

Согласована на портале № 82945

b) Сбой программного обеспечения;
c) Фальсификация, подделка документов;
d) Открытие электронного письма, содержащего вирус.

17. Территория вокруг помещений автоматизированной системы обработки данных, которая непрерывно контролируется персоналом или средствами автоматизированной системы обработки данных называется …
    a) Неконтролируемой зоной;
    b) Зоной помещений автоматизированной системы;
    c) Зоной баз данных защищаемой системы;
    d) Зоной контролируемой территории.
18. Угроза диверсии относится к …
    a) Субъективной преднамеренной причине нарушения целостности информации;
    b) Субъективной непреднамеренной причине нарушения целостности информации;
    c) Объективной непреднамеренной причине нарушения целостности информации;
    d) Объективной преднамеренной причине нарушения целостности информации.
19. Перехват данных является угрозой:
    a) Доступности;
    b) Конфиденциальности;
    c) Целостности;
    d) Достоверности.
20. Продолжите тезис верно: Класс задач «Легендирование» по защите информации…
    a) Не существует;
    b) Потерял актуальность в связи с переходом на новые стандарты симметричных криптосистем;
    c) Предполагает включение в состав элементов системы обработки информации дополнительных компонентов;
    d) Объединяет задачи по обеспечению получения злоумышленником искаженного представления о характере и предназначении объекта.
21. Риск информационной безопасности это
    a) Число уязвимостей в системе;
    b) Отношение стоимости системы защиты к вероятности её «простоя»;
    c) Сочетание вероятности угрозы информационной безопасности и последствий её наступления;
    d) Оценка стоимости защитных средств.
22. Совокупность условий и факторов, определяющих потенциальную или реально существующую опасность нарушения конфиденциальности, целостности, доступности информации называется …
    a) Угрозой безопасности;
    b) Компьютерной безопасностью;
    c) Анализом угроз;
    d) Атакой на информационную систему.
23. Что из перечисленного происходит при использовании RAID-массивов?
    a) Производится полное шифрование данных;
    b) Обеспечивается более высокий уровень защиты от вирусов;
    c) Повышается надёжность хранения данных;
    d) Увеличивается максимальная пропускная способность сети.
24. Заключительным этапом построения системы защиты является …
    a) Анализ уязвимых мест;
    b) Планирование;
    c) Обследование;
    d) Сопровождение.
25. Что из перечисленного не используется в биометрической аутентификации?
    a) Рисунок папиллярного узора;
    b) Клавиатурный почерк;
    c) Пластиковая карта с магнитной полосой;
    d) Радужная оболочка глаза.
26. К какой подсистеме не предъявляются требования в Руководящем документе

Согласована на портале № 82945

«Классификация автоматизированных систем и требований по защите информации»?
a) управления доступом;
b) регистрации и учета;
c) технической защиты информации;
d) обеспечения целостности.

27. Защита информации это:
a) Деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё;
b) Совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
c) Процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
d) Получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств.

28. Уровень безопасности С, согласно "Оранжевой книге", характеризуется:
a) Отсутствием управления доступом;
b) Произвольным управлением доступом;
c) Принудительным управлением доступом;
d) Верифицируемой безопасностью.

29. Свойство доступности достигается за счет применения мер, направленных на повышение:
a) Аутентичности;
b) Непротиворечивости;
c) Отказоустойчивости;
d) Неотказуемости.

30. Каким термином называется защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативнорозыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации?
a) Конфиденциальная информация;
b) Секретная информация;
c) Военная тайна;
d) Государственная тайна.

31. Получение доступа к информации субъектом в нарушение действующей политики разграничения доступа называется…
a) Несанкционированный доступ;
b) Злоумышленный доступ;
c) Неразрешенный доступ;
d) Запретный доступ.

32. Какой вид информации не относится к категории конфиденциальной информации?
a) Коммерческая тайна;
b) Тайна судопроизводства;
c) Персональные данные;
d) Государственная тайна.

33. Каким термином (согласно законодательству РФ) называется любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу?
a) Конфиденциальная информация;
b) Персональные данные;
c) Информация про личность;
d) Информация с ограниченным доступом.

34. Каналы несанкционированного получения информации сгруппированы в…
a) 3 класса;
b) 4 класса;
c) 7 классов;
d) 9 классов.

35. Набор норм, правил и практических приемов, регулирующих управление, защиту и

Согласована на портале № 82945

распространение ценной информации, называется …
a) Моделью безопасности;
b) Методом шифрования;
c) Компьютерной безопасностью;
d) Политикой безопасности.

36. Общая, руководящая установка при организации и обеспечении соответствующего вида деятельности, направленная на то, чтобы наиболее важные цели этой деятельности достигались при наиболее рациональном расходовании имеющихся ресурсов – это …
a) Миссия;
b) Стратегия;
c) Функция;
d) Процесс.

37. Что из перечисленного не является целью проведения аудита безопасности?
a) Анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов системы;
b) Выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности системы;
c) Оценка будущего уровня защищенности системы;
d) Оценка соответствия системы существующим стандартам в области информационной безопасности

38. Выберите неверное утверждение. Сигнатурный метод выявления атак характеризуется:
a) Сравнением исследуемого объекта с ранее известными образцами-эталонами;
b) Способностью обнаруживать ранее неизвестные атаки;
c) Простотой в настройке и эксплуатации для конечного пользователя системы;
d) Популярностью использования в системах антивирусной защиты.

39. Задачи по резервированию системы защиты делятся на:
a) Теплое и холодное резервирование;
b) Холодное и горячее резервирование;
c) Белое и серое резервирование;
d) Толстое и тонкое резервирование.

40. Модель системы с полным перекрытием характеризуется следующим положением:
a) В автоматизированной системе средствами защиты «перекрыто» большинство каналов утечки;
b) В механизме защиты должно содержаться по крайней мере одно средство для перекрытия любого потенциально возможного канала утечки информации;
c) В системе защиты присутствует только одно средство для перекрытия всех угроз безопасности;
d) Автоматизированная система является системой множественного доступа.

41. Инструментальная комплексность в сфере информационной безопасности подразумевает:
a) Непрерывность осуществления мероприятий по защите информации;
b) Защиту информации от внешних и внутренних угроз;
c) Интеграцию всех видов и направлений ИБ для достижения поставленных целей;
d) Обеспечение требуемого уровня защиты во всех элементах системы обработки информации.

42. Какой документ устанавливает цель, задачи и структуру стандартов по защите информации, объединяющий аспекты стандартизации в данной области и являющийся основополагающим стандартом в области защиты информации:
a) ГОСТ Р 52069.0-2013;
b) ФЗ №152 от 27.07.2006;
c) Постановление Правительства РФ №119 от 01.11.2012;
d) Конституция РФ.

43. Деятельность по подтверждению характеристик средств защиты информации требованиям государственных стандартов или иных нормативных документов по защите информации, утвержденных Государственной технической комиссией при Президенте Российской Федерации (Гостехкомиссией России) называется
a) Аттестация средств защиты информации;

Согласована на портале № 82945

b) Сертификация средств защиты информации;
c) Комплексное тестирование средств защиты информации;
d) Выборка средств защиты информации.

44. Положения Федерального закона №149 от 27.06.2006 не распространяются на:
a) Отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации;
b) Отношения, возникающие при применении информационных технологий;
c) Отношения, возникающие при обеспечении защиты информации;
d) Отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации.

9.1.2. Перечень вопросов для зачета

1. Основные регуляторы
2. Основные нормативно-правовые акты
3. Определения: информация, безопасность информации, защита информации, информационная безопасность, информационный процесс, документ, носитель
4. Свойства информации
5. Виды информации и их определения
6. Государственная тайна
7. Определения: угрозы, несанкционированный доступ.
8. Формы представления информации
9. Классификация угроз
10. Способы реализации угроз
11. Определения: защищаемая информация, доступ, допуск, уязвимость, СЗИ
12. Виды защиты информации
13. Конституционные основы в информационной сфере
14. Доктрина ИБ РФ (составляющие национальных интересов РФ)
15. ФЗ «Об информации, информационных технологиях и о защите информации»
16. Преступления в информационной сфере (УК)
17. Задачи организационного обеспечения ЗИ
18. Управление ИБ
19. Модель угроз и модель нарушителя
20. Сложности в работе с персоналом

9.1.3. 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

Согласована на портале № 82945

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 9.4.

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:

Согласована на портале № 82945

– 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 № 82945

ЛИСТ СОГЛАСОВАНИЯ

Рассмотрена и одобрена на заседании кафедры КИБЭВС
протокол № 11 от «24» 12 2024 г.

СОГЛАСОВАНО:

Должность	Инициалы, фамилия	Подпись
Заведующий выпускающей каф. ИРЭТ	А.М. Заболоцкий	Согласовано, 47c2d4ff-8c0e-484c-b856-20e4ba4f0e52
Заведующий обеспечивающей каф. КИБЭВС	А.А. Шелупанов	Согласовано, c53e145e-8b20-45aa-9347-a5e4dbb90e8d
Начальник учебного управления	И.А. Лариошина	Согласовано, c3195437-a02f-4972-a7c6-ab6ee1f21e73

ЭКСПЕРТЫ:

Директор, каф. ИРЭТ	А.М. Заболоцкий	Согласовано, 47c2d4ff-8c0e-484c-b856-20e4ba4f0e52
Доцент, каф. КИБЭВС	А.А. Конев	Согласовано, 81687a04-85ce-4835-9e1e-9934a6085fdd

РАЗРАБОТАНО:

Доцент, каф. КИБЭВС	А.Ю. Якимук	Разработано, 4ffdf265-fb78-4863-b293-f03438cb07cc

Согласована на портале № 82945