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

ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **38.05.01 Экономическая безопасность**
Направленность (профиль) / специализация: **Экономико-правовое обеспечение экономической безопасности**
Форма обучения: **очная**
Факультет: **Факультет безопасности (ФБ)**
Кафедра: **Кафедра комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)**
Курс: **3**
Семестр: **5**
Учебный план набора 2021 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	5 семестр	Всего	Единицы
Лекционные занятия	40	40	часов
Практические занятия	28	28	часов
Самостоятельная работа	40	40	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	5

Томск

1. Общие положения

1.1. Цели дисциплины

1. дать основы правового обеспечения информационной безопасности, а также формирование знаний по организационному обеспечению информационной безопасности и навыков по их определению для конкретных условий.

1.2. Задачи дисциплины

1. дать основы законодательства РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации.
2. дать основы понятий и видов защищаемой информации по законодательству РФ.
3. дать основы правовых режимов конфиденциальной информации.
4. дать основы правового режим защиты государственной тайны, системы защиты государственной тайны.
5. дать основы лицензирования и сертификации в области защиты информации, в том числе государственной тайны.
6. дать основы правовых основ защиты информации с использованием технических средств (защита от технических разведок, применение и разработка шифровальных средств, электронная цифровая подпись и т.д.).
7. дать основы защиты интеллектуальной собственности.
8. дать основы правовой регламентации охранной деятельности.
9. дать основы правового регулирования взаимоотношений администрации и персонала в области защиты информации.
10. дать основы международного законодательства в области защиты информации.
11. дать основы знаний о преступлениях в сфере компьютерной информации, экспертизах преступлений в области компьютерной информации, криминалистических аспектах проведения расследований.
12. дать основы угроз информационной безопасности объекта.
13. дать основы организации службы безопасности объекта.
14. дать основы подбора и работы с кадрами в сфере информационной безопасности.
15. дать основы организации и обеспечения режима конфиденциальности.
16. дать основы охраны объектов.

2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).
Часть блока дисциплин: Обязательная часть.
Модуль дисциплин: Модуль специальности (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		

ОПК-5. Способен осуществлять профессиональную деятельность в соответствии с нормами профессиональной этики, нормами права, нормативными правовыми актами в сфере экономики, исключающими противоправное поведение	ОПК-5.1. Знает основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области экономической безопасности	Знает основные виды и порядок применения нормативных и методических документов, а также порядок соблюдения законодательных ограничений в сфере профессиональной деятельности
	ОПК-5.2. Умеет формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации	Умеет использовать основные методы правовой оценки различных подходов решения задач в сфере профессиональной деятельности
	ОПК-5.3. Владеет навыками информационно-аналитического обеспечения предупреждения, выявления, пресечения, раскрытия и расследования экономических и налоговых преступлений	Владеет навыками разработки текстовой документации в области профессиональной деятельности в соответствии с нормативными требованиями, регламентирующими деятельность по защите информации
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
		5 семестр
Контактная аудиторная работа обучающихся с преподавателем, всего	68	68
Лекционные занятия	40	40
Практические занятия	28	28
Самостоятельная работа обучающихся, в т.ч. контактная внеаудиторная работа обучающихся с преподавателем, всего	40	40
Подготовка к тестированию	40	40
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	Прак. зан., ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
5 семестр					
1 Законодательство РФ в области информационной безопасности.	4	-	4	8	ОПК-5
2 Правовые основы защиты конфиденциальной информации.	6	4	4	14	ОПК-5
3 Правовые основы защиты государственной тайны.	4	4	4	12	ОПК-5
4 Лицензирование и сертификация.	4	-	4	8	ОПК-5
5 Нормы ответственности за правонарушения в сфере компьютерных технологий.	4	4	4	12	ОПК-5
6 Анализ объекта защиты с позиции организационного обеспечения информационной безопасности.	4	4	4	12	ОПК-5
7 Средства и методы физической защиты объектов.	4	4	4	12	ОПК-5
8 Организация службы безопасности и работа с кадрами.	4	4	4	12	ОПК-5
9 Организация и обеспечения режима секретности.	2	2	4	8	ОПК-5
10 Организация пропускного и внутри объектового режима.	4	2	4	10	ОПК-5
Итого за семестр	40	28	40	108	
Итого	40	28	40	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
5 семестр			
1 Законодательство РФ в области информационной безопасности.	Понятие и структура информационной безопасности. Основные задачи системы информационной безопасности. Законодательство РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации. Субъекты и объекты правоотношений в области информационной безопасности. Отрасли законодательства, регламентирующие деятельность по защите информации.	4	ОПК-5
	Итого	4	

2 Правовые основы защиты конфиденциальной информации.	Конфиденциальная информация. Виды тайн. Коммерческая тайна. Профессиональные тайны. Служебная тайна. Персональные данные. Тайна следствия и судопроизводства. Банковская тайна. Тайна телефонных переговоров и переписки.	6	ОПК-5
	Итого	6	
3 Правовые основы защиты государственной тайны.	Государственная тайна, как особый вид защищаемой информации и ее характерные признаки. Реквизиты носителей сведений, составляющих государственную тайну. Принципы, механизмы и процедура отнесения сведений к государственной тайне, их засекречивание и рассекречивание. Система защиты государственной тайны. Органы защиты государственной тайны и их компетенции. Порядок допуска и доступ к государственной тайне. Перечень и содержание организационных мер, направленных на защиту государственной тайны.	4	ОПК-5
	Итого	4	
4 Лицензирование и сертификация.	Правовая основа лицензирования и сертификации в области защиты информации, в том числе защиты государственной тайны. Виды деятельности в информационной сфере, подлежащие лицензированию. Лицензирование деятельности по защите информации.	4	ОПК-5
	Итого	4	
5 Нормы ответственности за правонарушения в сфере компьютерных технологий.	Уголовно-правовые нормы. Основные принципы и понятия уголовного права. Преступления в сфере компьютерной информации. Экспертиза компьютерных преступлений. Административные правонарушения.	4	ОПК-5
	Итого	4	

6 Анализ объекта защиты с позиции организационного обеспечения информационной безопасности.	Задачи организационного обеспечения информационной безопасности. Роль нормативных документов в защите информации. Инвентаризация информационных ресурсов организации. Построение моделей документооборота и информационных систем. Модели нарушителя информационной безопасности. Анализ и оценка угроз информационной безопасности объекта. Оценка ущерба вследствие противоправного выхода информации ограниченного доступа из защищаемой сферы и меры по его локализации.	4	ОПК-5
	Итого	4	
7 Средства и методы физической защиты объектов.	Структура системы физической защиты. Система охраны периметра. Система сигнализации, видеонаблюдения, контроля доступа: классификация, сферы применения.	4	ОПК-5
	Итого	4	
8 Организация службы безопасности и работа с кадрами.	Служба безопасности объекта. Принципы деятельности службы безопасности. Задачи и функции службы безопасности. Структура службы безопасности. Функции сотрудников службы безопасности. Контроль состояния системы защиты, проведение служебных расследований. Подбор, расстановка и работа с кадрами. Внутренние угрозы информационной безопасности, социальная инженерия. Функции службы безопасности при подборе, увольнении сотрудников и текущей работе с ними. Нормативное обеспечение работы сотрудников организации с информацией ограниченного доступа.	4	ОПК-5
	Итого	4	

9 Организация и обеспечения режима секретности.	Основные принципы организации и обеспечения секретного документооборота. Технологические меры поддержания информационной безопасности объектов. Организация совещания и переговоров. Регламентация предоставления сотрудникам допуска к информации ограниченного доступа. Регламентация выдачи (возврата) документов и работы с ними. Регламентация процедуры создания документа ограниченного доступа. Регламентация процедуры снятие грифа с документов ограниченного доступа и их уничтожения. Регламентация обмена документами с другими организациями. Обеспечение информационной безопасности объекта (учреждения, банка, промышленного предприятия) при осуществлении международного научнотехнического и экономического сотрудничества. Организация режима и охраны объектов в процессе транспортировки.	2	ОПК-5
	Итого	2	
10 Организация пропускного и внутри объектового режима.	Проектирование пропускного и внутри объектового режима. Категорирование помещений. Регламентация пропуска лиц в здания. Виды пропусков и порядок их оформления. Порядок пропуска автотранспорта на территорию организации. Регламентация приема и сдачи объекта под охрану. Защита информации при авариях, иных экстремальных ситуациях и в условиях чрезвычайного положения. Структура аварийного плана.	4	ОПК-5
	Итого	4	
	Итого за семестр	40	
	Итого	40	

5.3. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 5.3.

Таблица 5.3 – Наименование практических занятий (семинаров)

Названия разделов (тем) дисциплины	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
5 семестр			
2 Правовые основы защиты конфиденциальной информации.	Работа с конфиденциальной информацией. Защита коммерческой тайны.	4	ОПК-5
	Итого	4	

3 Правовые основы защиты государственной тайны.	Работа с государственной тайной.	4	ОПК-5
	Итого	4	
5 Нормы ответственности за правонарушения в сфере компьютерных технологий.	Нарушение законодательства в сфере информационных технологий. Компьютерные преступления.	4	ОПК-5
	Итого	4	
6 Анализ объекта защиты с позиции организационного обеспечения информационной безопасности.	Описание структуры защищаемой организации и видов защищаемой информации.	4	ОПК-5
	Итого	4	
7 Средства и методы физической защиты объектов.	Определение угроз автоматизированной системе, обрабатывающей информацию ограниченного доступа, и требований к работе сотрудника с этой информацией.	4	ОПК-5
	Итого	4	
8 Организация службы безопасности и работа с кадрами.	Разработка структуры службы безопасности организации.	4	ОПК-5
	Итого	4	
9 Организация и обеспечения режима секретности.	Выбор способов и методов защиты информации и автоматизированной системы.	2	ОПК-5
	Итого	2	
10 Организация пропускного и внутри объектового режима.	Проектирование пропускного и внутри объектового режима в организации.	2	ОПК-5
	Итого	2	
	Итого за семестр	28	
	Итого	28	

5.4. Лабораторные занятия

Не предусмотрено учебным планом

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
5 семестр				
1 Законодательство РФ в области информационной безопасности.	Подготовка к тестированию	4	ОПК-5	Тестирование
	Итого	4		

2 Правовые основы защиты конфиденциальной информации.	Подготовка к тестированию	4	ОПК-5	Тестирование
	Итого	4		
3 Правовые основы защиты государственной тайны.	Подготовка к тестированию	4	ОПК-5	Тестирование
	Итого	4		
4 Лицензирование и сертификация.	Подготовка к тестированию	4	ОПК-5	Тестирование
	Итого	4		
5 Нормы ответственности за правонарушения в сфере компьютерных технологий.	Подготовка к тестированию	4	ОПК-5	Тестирование
	Итого	4		
6 Анализ объекта защиты с позиции организационного обеспечения информационной безопасности.	Подготовка к тестированию	4	ОПК-5	Тестирование
	Итого	4		
7 Средства и методы физической защиты объектов.	Подготовка к тестированию	4	ОПК-5	Тестирование
	Итого	4		
8 Организация службы безопасности и работа с кадрами.	Подготовка к тестированию	4	ОПК-5	Тестирование
	Итого	4		
9 Организация и обеспечения режима секретности.	Подготовка к тестированию	4	ОПК-5	Тестирование
	Итого	4		
10 Организация пропускного и внутри объектового режима.	Подготовка к тестированию	4	ОПК-5	Тестирование
	Итого	4		
Итого за семестр		40		
	Подготовка и сдача экзамена	36		Экзамен
Итого		76		

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.	Прак. зан.	Сам. раб.	
ОПК-5	+	+	+	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
5 семестр				
Тестирование	20	20	30	70
Экзамен				30
Итого максимум за период	20	20	30	100
Нарастающим итогом	20	40	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. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс]: учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. —Москва : Издательство Юрайт, 2021. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [Электронный ресурс]: — Режим доступа: https://urait.ru/bcode/469235.

7.2. Дополнительная литература

1. ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ ПРИКАЗ 11 февраля 2013 г. N 17 ОБ УТВЕРЖДЕНИИ ТРЕБОВАНИЙ О ЗАЩИТЕ ИНФОРМАЦИИ, НЕ СОСТАВЛЯЮЩЕЙ ГОСУДАРСТВЕННУЮ ТАЙНУ, СОДЕРЖАЩЕЙСЯ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ [Электронный ресурс]: — Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/110-prikazy/702-prikaz-fstek-rossii-ot11-fevralya-2013-g-n-17.

2. ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ МЕТОДИЧЕСКИЙ ДОКУМЕНТ МЕТОДИКА ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ [Электронный ресурс]: — Режим доступа: https://fstec.ru/tekhnicheskaya-zashchitainformatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokumentutverzhden-fstek-rossii-5-fevralya-2021-g.

3. ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ Утвержден ФСТЭК России 11 февраля 2014 г. МЕТОДИЧЕСКИЙ ДОКУМЕНТ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ [Электронный ресурс]: — Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/805-metodicheskij-dokument.

7.3. Учебно-методические пособия

7.3.1. Обязательные учебно-методические пособия

1. Организационно-правовое обеспечение информационной безопасности: Методические указания по практическим занятиям и самостоятельной работе / Э. В. Семенов - 2012. 13 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/2506.

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 практических занятий

Аудитория Интернет-технологий и информационно-аналитической деятельности: учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа; 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 402 ауд.

Описание имеющегося оборудования:

- Интерактивная доска IQBoard DVT TN100;
- Проектор Optoma EH400;
- Веб-камера Logitech C920s;
- Акустическая система Yamaha;
- Комплект беспроводных микрофонов Clevermic;
- Магнитно-маркерная доска;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- Microsoft Windows 10;
- VirtualBox;

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 Законодательство РФ в области информационной безопасности.	ОПК-5	Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
2 Правовые основы защиты конфиденциальной информации.	ОПК-5	Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
3 Правовые основы защиты государственной тайны.	ОПК-5	Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
4 Лицензирование и сертификация.	ОПК-5	Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
5 Нормы ответственности за правонарушения в сфере компьютерных технологий.	ОПК-5	Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
6 Анализ объекта защиты с позиции организационного обеспечения информационной безопасности.	ОПК-5	Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
7 Средства и методы физической защиты объектов.	ОПК-5	Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
8 Организация службы безопасности и работа с кадрами.	ОПК-5	Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
9 Организация и обеспечения режима секретности.	ОПК-5	Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
10 Организация пропускного и внутри объектового режима.	ОПК-5	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. Вопрос 1 Что такое информация в соответствии с Федеральным законом №149-ФЗ?
   Сообщения и данные
   Изображения
   Сведения об интеллектуальной собственности
   Сведения (сообщения, данные) независимо от формы их представления
2. Вопрос 2 Дата принятия Конституции Российской федерации?
   01 января 1991
   10 декабря 1992
   12 декабря 1993
   15 ноября 1994
3. Вопрос 3 Конфиденциальность информации это?
   Целостность и доступность информации при ее обработке в автоматизированных системах управления технологическими процессами.
   Сохранность персональных данных субъекта персональных данных при попытках доступа третьих лиц в информационную систему персональных данных.
   Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.
   Обязательно требование для выполнения лицом, получившим доступа к сведениям, содержащим государственную тайну.
4. Вопрос 4 Обладатель информации это?
   Лицо, оформившее права на интеллектуальную собственность в соответствии с законодательством Российской Федерации об интеллектуальной собственности.
   Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.
   Юридическое лицо, оформляющее право на интеллектуальную собственность физических лиц и юридических лиц за исключением резидентов иностранных государств.
   Юридическое лицо, зарегистрированное за пределами Российской Федерации и регистрирующее право интеллектуальной собственности на территории Российской Федерации.
5. Вопрос 5 Дата принятия Доктрины информационной безопасности Российской Федерации?
   21 июля 1993
   09 сентября 2000
   27 июня 2006
   05 декабря 2016
6. Вопрос 6 Обеспечение информационной безопасности в соответствии с Доктриной информационной безопасности Российской Федерации?
   Совокупность правовых, организационно-технических и экономических методов.
   Совокупность правовых, организационных и технических методов.
   Совокупность оперативно-розыскных, научно-технических, информационно-аналитических мер.
   Совокупность оперативно-розыскных, научно-технических, информационно-аналитических и иных мер.
7. Вопрос 7 Основные компоненты справочно-правовой системы?
   Программная оболочка, экспертная группа юристов.
   Программная оболочка, информационный банк.
   Информационный банк, техническая поддержка.
   Техническая поддержка, экспертная группа правоведов.

8. Вопрос 8 Каким образом делиться информация по категориям доступа?
   Государственная тайна и персональные данные.
   Общедоступная информация и информация ограниченного доступа.
   Служебная тайна и адвокатская тайна.
   Конфиденциальная информация и государственная тайна.
9. Вопрос 9 Пометка коммерческая тайна содержит:
   Фамилия, имя, отчество индивидуального предпринимателя.
   Наименование юридического лица.
   Место нахождения юридического лица.
   Наименование и место нахождения юридического лица.
10. Вопрос 10 Режим коммерческой тайны считается установленным?
    После устного распоряжения генерального директора.
    После собрания совета директоров юридического лица.
    После письменного распоряжения уполномоченного лица.
    После назначения лица, ответственного за защиту коммерческой тайны.
11. Вопрос 11 Какое количество типов актуальных угроз персональным данным описывается в постановлении Правительства РФ от 01.11.2012 №1119?
    Один
    Два
    Три
    Четыре
12. Вопрос 12 Контроль за выполнением требований к защите персональных данных, утвержденный постановлением Правительства РФ от 01.11.2012 №1119 выполняется не реже чем 1 раз в:
    1 год
    3 года
    5 лет
    На усмотрение оператора персональных данных
13. Вопрос 13 Постановление Правительства РФ от 01.11.2012 №1119 устанавливает:
    Классы защищенности персональных данных
    Уровни защищенности персональных данных
    Уровни значимости персональных данных
    Все выше перечисленное
14. Вопрос 14 Выбор класса средств криптографической защиты информации в соответствии с приказом ФСБ от 10.07.2014 №378 основывается на:
    Модели актуальных угроз персональных данных
    Типе актуальных угроз персональных данных
    Уровне защищенности персональных данных
    Ни один из выше перечисленных пунктов
15. Вопрос 15 Какое минимальное число сотрудников устанавливает постановление Правительства от 03.02.2012 №79 соискателю лицензии на деятельность по технической защите конфиденциальной информации (не содержащей сведения, составляющие государственную тайну) являющемуся юридическим лицом:
    1 сотрудник
    2 сотрудника
    3 сотрудника
    5 сотрудников
16. Вопрос 16 Какие требования к работникам соискателя лицензии на деятельность по технической защите конфиденциальной информации (не содержащей сведения, составляющие государственную тайну) предъявляет постановление Правительства от 03.02.2012 №79:
    Работа в штате по основному месту работы
    Работа в штате по внешнему совместительству и высшее образование по направлению подготовки (специальности) в области информационной безопасности и стаж работы в области проводимых работ по лицензируемому виду деятельности не менее 3 лет
    Высшее образование и стаж работы в области проводимых работ по лицензируемому виду деятельности не менее 3 лет, прошедших обучение по программам

профессиональной переподготовки по одной из специальностей в области информационной безопасности
Работа в штате по основному месту работы и высшее образование по направлению подготовки (специальности) в области математических и естественных наук, инженерного дела, технологий и технических наук и стаж работы в области проводимых работ по лицензируемому виду деятельности не менее 5 лет

17. Вопрос 17 Для выполнения работ и услуг по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации лицензиат ФСТЭК должен иметь в наличии:
Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11.02.2013 N 17 и ГОСТ 2.103-2013 ЕСКД Стадии разработки
Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11.02.2013 N 17 и ГОСТ 2.119-2013 ЕСКД Эскизный проект
ГОСТ 2.503-2013 ЕСКД Правила внесения изменений и ГОСТ 2.610-2006 ЕСКД Правила выполнения эксплуатационных документов
ГОСТ Р 8.563-2009 Государственная система обеспечения единства измерений. Методики (методы) измерений и ГОСТ 28195-89 Оценка качества программных средств. Общие положения
18. Вариант 18 Для выполнения работ мониторингу информационной безопасности средств и систем информатизации лицензиат ФСТЭК должен иметь в наличии:
Средства управления информацией об угрозах безопасности информации
Программные средства контроля целостности
Программные средства формирования и контроля полномочий доступа в информационных (автоматизированных) системах
Осциллографы
19. Вопрос 19 Для какого вида деятельности в соответствии с постановление Правительства от 16.04.2012 №313 не требуется получение лицензии:
Монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств информационных систем
Монтаж шифровальных (криптографических) средств, предназначенных для защиты информации, содержащей сведения, составляющие государственную тайну
Монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем
Изготовление и распределение ключевых документов и (или) исходной ключевой информации для выработки ключевых документов с использованием аппаратных, программных и программно-аппаратных средств, систем и комплексов изготовления и распределения ключевых документов для шифровальных (криптографических) средств
20. Вопрос 20 Какое требование предъявляется к руководителю и (или) лицу, уполномоченное руководить работами по модернизации шифровальных (криптографических) средств
Высшее профессиональное образование по направлению подготовки "Информационная безопасность" и (или) прошедшие переподготовку по одной из специальностей этого направления (нормативный срок - свыше 1000 аудиторных часов), а также имеющие стаж в области выполняемых работ в рамках лицензируемой деятельности не менее 3 лет
Высшее профессиональное образование по направлению подготовки "Информационная безопасность" и (или) прошедшие переподготовку по одной из специальностей этого направления (нормативный срок - свыше 500 аудиторных часов), а также имеющие стаж в области выполняемых работ в рамках лицензируемой деятельности не менее 5 лет
Высшее профессиональное образование по направлению подготовки "Информационная безопасность" и (или) прошедшие переподготовку по одной из специальностей этого направления (нормативный срок - свыше 1000 аудиторных часов), а также имеющие стаж в области выполняемых работ в рамках лицензируемой деятельности не менее 5 лет
Любой из перечисленных пунктов
21. Вопрос 21 Какое требование предъявляется к руководителю и (или) лицу, уполномоченное руководить работами по передаче шифровальных (криптографических)

средств, за исключением шифровальных (криптографических) средств защиты фискальных данных, разработанных для применения в составе контрольно-кассовой техники, сертифицированных Федеральной службой безопасности Российской Федерации
Высшее профессиональное образование по направлению подготовки "Информационная безопасность" и (или) прошедшие переподготовку по одной из специальностей этого направления (нормативный срок - свыше 1000 аудиторных часов), а также имеющие стаж в области выполняемых работ в рамках лицензируемой деятельности не менее 3 лет
Высшее профессиональное образование по направлению подготовки "Информационная безопасность" и (или) прошедшие переподготовку по одной из специальностей этого направления (нормативный срок - свыше 500 аудиторных часов), а также имеющие стаж в области выполняемых работ в рамках лицензируемой деятельности не менее 5 лет
Высшее профессиональное образование по направлению подготовки "Информационная безопасность" и (или) прошедшие переподготовку по одной из специальностей этого направления (нормативный срок - свыше 1000 аудиторных часов), а также имеющие стаж в области выполняемых работ в рамках лицензируемой деятельности не менее 5 лет
Любой из перечисленных пунктов

22. Вопрос 22 Какие организации создают свои системы сертификации средств защиты информации?
Федеральная служба безопасности Российской Федерации
Федеральная служба по техническому и экспортному контролю Российской Федерации
Министерство обороны Российской Федерации
Все вышеперечисленные
23. Вопрос 23 Какие из перечисленных функций не входят в перечень компетенций федерального органа по сертификации?
выдает сертификаты и лицензии на применение знака соответствия
приостанавливает или отменяет действие выданных сертификатов
формируют фонд нормативных документов, необходимых для сертификации
организует работы по формированию системы сертификации и руководство ею, координирует деятельность органов по сертификации средств защиты информации и испытательных лабораторий, входящих в систему сертификации
24. Вопрос 24 В компетенцию какого ведомства входит сертификация средств криптографической защиты информации?
Федеральная служба безопасности Российской Федерации
Федеральная служба по техническому и экспортному контролю Российской Федерации
Министерство обороны Российской Федерации
Все вышеперечисленные
25. Вопрос 25 В каком случае аттестация объекта информатизации является добровольной?
обработка государственной тайны
при защите государственного информационного ресурса
управление экологически опасными объектами
ведение конфиденциальных переговоров
26. Вопрос 26 Кто создает организационную структуру системы аттестации объектов информатизации по требованиям безопасности информации
Федеральная служба безопасности Российской Федерации
Федеральная служба по техническому и экспортному контролю Российской Федерации
Министерство обороны Российской Федерации
Все вышеперечисленные
27. Вопрос 27 Какое действие не является обязательным при аттестации объектов информатизации по требованиям безопасности информации
подачу и рассмотрение заявки на аттестацию
разработка программы и методики аттестационных испытаний
испытание несертифицированных средств и систем защиты информации
оформление, регистрация и выдача "Аттестата соответствия"
28. Вопрос 28 Максимальный срок действия аттестата объекта информатизации в соответствии с "Положение по аттестации объектов информатизации по требованиям безопасности информации" утвер - жденного Гостехкомиссией РФ от 25.11.1994
1 год

2,5 года
3 года
5 лет

29. Вопрос 29 Какое постановление Правительства РФ регламентирует лицензирование деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну?
Постановление Правительства РФ от 03.02.2012 N 79
Постановление Правительства РФ от 16.04.2012 N 313
Постановление Правительства РФ от 12.04.2012 N 287
Постановление Правительства РФ от 15.04.1995 N 333
30. Вопрос 30 Чем является защита государственной тайны?
видом основной деятельности
совокупностью органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну и их носителей, а также мероприя - тий, проводимых в этих целях
техническими, криптографическими, программными и другими средствами, предназначенными для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средствами контроля эффективности защиты информации
процедурой оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций - на проведение работ с использованием таких сведений

9.1.2. Перечень экзаменационных вопросов

1. Законодательство РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации.
2. Конституционные гарантии прав граждан на информацию и механизм их реализации.
3. Понятие и виды защищаемой информации по законодательству РФ.
4. Государственная тайна как особый вид защищаемой информации.
5. Конфиденциальная информация.
6. Система защиты государственной тайны.
7. Правовой режим защиты государственной тайны.
8. Правовое регулирование взаимоотношений администрации и персонала в области защиты информации.
9. Правовые режимы конфиденциальной информации.
10. Лицензирование и сертификация в области защиты информации, в том числе государственной тайны.
11. Правовые основы защиты информации с использованием технических средств (защита от технических разведок, применение и разработка шифровальных средств, электронная цифровая подпись и т.д.).
12. Защита интеллектуальной собственности.
13. Правовая регламентация охранной деятельности.
14. Международное законодательство в области защиты информации.
15. Преступления в сфере компьютерной информации.
16. Экспертиза преступлений в области компьютерной информации.
17. Криминалистические аспекты проведения расследований.

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 КИБЭВС
протокол № 5 от « 5 » 5 2021 г.

СОГЛАСОВАНО:

Должность	Инициалы, фамилия	Подпись
Заведующий выпускающей каф. КИБЭВС	А.А. Шелупанов	Согласовано, c53e145e-8b20-45aa-9347-a5e4dbb90e8d
Заведующий обеспечивающей каф. КИБЭВС	А.А. Шелупанов	Согласовано, c53e145e-8b20-45aa-9347-a5e4dbb90e8d
Начальник учебного управления	Е.В. Саврук	Согласовано, fa63922b-1fce-4a6a-845d-9ce7670b004c

ЭКСПЕРТЫ:

Доцент, каф. КИБЭВС	А.А. Конев	Согласовано, 81687a04-85ce-4835-9e1e-9934a6085fdd
Доцент, каф. КИБЭВС	К.С. Сарин	Согласовано, 68c81ca0-0954-467a-8d01-f93a0d553669

РАЗРАБОТАНО:

Доцент, каф. КИБЭВС	Е.Ю. Костюченко	Разработано, c6235dfe-234a-4234-88f9-e1597aac6463