МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Проректор по УР
_____Сенченко П.В.
«18» _____02_____ 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОРГАНИЗАЦИЯ ЗАЩИТЫ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Уровень образования: **высшее образование - магистратура**
Направление подготовки / специальность: **10.04.01 Информационная безопасность**
Направленность (профиль) / специализация: **Информационная безопасность объектов критической информационной инфраструктуры**
Форма обучения: **очная**
Факультет: **Факультет безопасности (ФБ)**
Кафедра: **Кафедра комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)**
Курс: **1**
Семестр: **2**
Учебный план набора 2023 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	2 семестр	Всего	Единицы
Лекционные занятия	16	16	часов
Практические занятия	32	32	часов
в т.ч. в форме практической подготовки	24	24	часов
Самостоятельная работа	60	60	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	2

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Сенченко П.В.
Должность: Проректор по УР
Дата подписания: 18.02.2022
Уникальный программный ключ:
a1119608-cdff-4455-b54e-5235117c185c

Томск

Согласована на портале № 73593

1. Общие положения

1.1. Цели дисциплины

1. Формирование компетенций, необходимых специалистам, для обеспечения безопасности значимых объектов критической инфраструктуры.

1.2. Задачи дисциплины

1. Выделение объектов, угроз, определение способов и средств защиты объектов критической инфраструктуры.
2. Освоение на практике специфики проведения комплекса мероприятий по определению оснований для отнесения организации к объектам критической информационной инфраструктуры.
3. Изучение особенностей проведения инвентаризации и категорирования объектов критической информационной инфраструктуры.

2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).
Часть блока дисциплин: Часть, формируемая участниками образовательных отношений.
Модуль дисциплин: Модуль профессиональной подготовки (major).
Индекс дисциплины: Б1.В.1.3.
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		

Согласована на портале № 73593

УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1. Знает методики сбора и обработки информации, актуальные российские и зарубежные источники информации для решения поставленных задач, а также методы системного анализа	Знает основные источники информации о проблемных ситуациях на объектах критической информационной инфраструктуры и ее частях, а также подходы к критическому анализу этой информации.
	УК-1.2. Умеет применять методики поиска, сбора и обработки информации, осуществлять критический анализ и синтез информации, полученной из разных источников	Знает порядок принятия решений при возникновении проблемных ситуаций на объектах критической информационной инфраструктуры и ее частях.
	УК-1.3. Владеет методами поиска, сбора и обработки, критического анализа и синтеза информации, методикой системного подхода для решения поставленных задач; способен генерировать различные варианты решения поставленных задач	Владеет методами поиска, сбора и обработки, критического анализа и синтеза информации, методикой системного подхода для организации защиты объектов критической информационной инфраструктуры и ее частей, а также способен генерировать различные варианты решения поставленных задач.
УК-2. Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1. Знает основные модели жизненного цикла проекта, его этапы и фазы, их характеристики и особенности	Знает основные модели жизненного цикла объектов критической информационной инфраструктуры и ее частей, их характеристики и особенности.
	УК-2.2. Умеет разрабатывать и реализовывать этапы проекта в сфере профессиональной деятельности	Умеет разрабатывать и реализовывать этапы проекта по организации защиты объектов критической информационной инфраструктуры и ее частей.
	УК-2.3. Имеет навыки работы в области проектной деятельности и реализации проектов	Имеет навыки разработки и реализации этапов проекта по организации защиты объектов критической информационной инфраструктуры и ее частей.
Общепрофессиональные компетенции		
-	-	-
Профессиональные компетенции		

Согласована на портале № 73593

ПК-1. Способен обеспечивать анализ, проектирование, разработку, функционирование, эксплуатацию систем информационной безопасности объектов критической информационной инфраструктуры и ее частей;	ПК-1.1. Знает общие принципы проектирования систем информационной безопасности объектов критической информационной инфраструктуры и ее частей, принципы построения систем информационной безопасности объектов критической информационной инфраструктуры и ее частей, состав технико-экономического обоснования проектируемых систем информационной безопасности объектов критической информационной инфраструктуры и ее частей	Знает общие принципы организации защиты объектов критической информационной инфраструктуры и ее частей.
	ПК-1.2. Умеет разрабатывать необходимую техническую документацию в области проектирования систем информационной безопасности объектов критической информационной инфраструктуры и ее частей с учетом действующих нормативных и методических документов, проводить подготовку исходных данных для технико-экономического обоснования проектируемых систем информационной безопасности объектов критической информационной инфраструктуры и ее частей	Умеет организовывать защиту объектов критической информационной инфраструктуры и ее частей с учетом действующих нормативных и методических документов;
	ПК-1.3. Владеет навыками проектирования элементов систем информационной безопасности объектов критической информационной инфраструктуры	Определяет категории объектов критической информационной инфраструктуры.

Согласована на портале № 73593

ПК-3. Способен разрабатывать организационно-распорядительные документы, регламентирующие функционирование систем информационной безопасности объектов критической информационной инфраструктуры	ПК-3.1. Знает содержание и порядок деятельности персонала по эксплуатации систем информационной безопасности объектов критической информационной инфраструктуры	Знает содержание и порядок деятельности персонала объектов критической информационной инфраструктуры и ее частей.
	ПК-3.2. Знает нормативную базу, регламентирующую процессы проектирования, построения и эксплуатации систем информационной безопасности объектов критической информационной инфраструктуры	Знает нормативную базу, регламентирующую процессы обеспечения информационной безопасности объектов критической информационной инфраструктуры и ее частей.
	ПК-3.3. Умеет разрабатывать технические задания на создание систем информационной безопасности объектов критической информационной инфраструктуры с учетом действующих нормативных и методических документов	Умеет разрабатывать организационно-распорядительные документы по обеспечению безопасности значимых объектов критической информационной инфраструктуры.
	ПК-3.4. Владеет инструментами проведения и фиксации результатов проверки функционирования систем информационной безопасности объектов критической информационной инфраструктуры	Владеет техническими мерами обеспечения безопасности значимых объектов критической информационной инфраструктуры.
	ПК-3.5. Умеет осуществлять планирование и организацию работы персонала систем информационной безопасности объектов критической информационной инфраструктуры с учетом требований по защите информации.	Умеет осуществлять организацию работы персонала систем информационной безопасности объектов критической информационной инфраструктуры с учетом требований по защите информации.

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.

Согласована на портале № 73593

Таблица 4.1 – Трудоемкость дисциплины по видам учебной деятельности

Виды учебной деятельности	Всего часов	Семестры
		2 семестр
Контактная аудиторная работа обучающихся с преподавателем, всего	48	48
Лекционные занятия	16	16
Практические занятия	32	32
Самостоятельная работа обучающихся, в т.ч. контактная внеаудиторная работа обучающихся с преподавателем, всего	60	60
Написание конспекта самоподготовки	8	8
Подготовка к тестированию	10	10
Подготовка к устному опросу / собеседованию	10	10
Написание отчета по практическому занятию (семинару)	32	32
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
2 семестр					
1 Понятие критической информационной инфраструктуры	2	2	5	9	ПК-1, ПК-3, УК-1, УК-2
2 Правовое обеспечение критической информационной инфраструктуры	4	4	12	20	ПК-1, ПК-3, УК-1, УК-2
3 Категории объектов критической информационной инфраструктуры	2	8	12	22	ПК-1, ПК-3, УК-1, УК-2
4 Технические и организационные меры безопасности значимых объектов	4	6	12	22	ПК-1, ПК-3, УК-1, УК-2
5 Модели угроз и выбор мер защиты объектов критической информационной инфраструктуры	2	8	12	22	ПК-1, ПК-3, УК-1, УК-2
6 Организационно-распорядительные документы по обеспечению безопасности значимых объектов критической информационной инфраструктуры	2	4	7	13	ПК-1, ПК-3, УК-1, УК-2
Итого за семестр	16	32	60	108	
Итого	16	32	60	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

Согласована на портале № 73593

2 семестр			
1 Понятие критической информационной инфраструктуры	Термины и определения, понятие критической информационной инфраструктуры (КИИ), объекты КИИ	2	ПК-1, ПК-3, УК-1, УК-2
	Итого	2	
2 Правовое обеспечение критической информационной инфраструктуры	Документы, определяющие регулирование отношений в области обеспечения безопасности КИИ. Оценка безопасности КИИ. Государственный контроль в области обеспечения безопасности значимых объектов КИИ.	4	ПК-1, ПК-3, УК-1, УК-2
	Итого	4	
3 Категории объектов критической информационной инфраструктуры	Классификация АСУТП. Критерии значимости объектов КИИ РФ и их значения. Сведения об объекте КИИ и угрозах ИБ. Нарушители ИБ объектов КИИ. Организационные и технические меры, применяемые для обеспечения ИБ КИИ.	2	ПК-1, ПК-3, УК-1, УК-2
	Итого	2	
4 Технические и организационные меры безопасности значимых объектов	Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры. Анализ угроз и разработка модели угроз. Проектирование системы безопасности значимого объекта КИИ. Разработка рабочей и эксплуатационной документации	4	ПК-1, ПК-3, УК-1, УК-2
	Итого	4	
5 Модели угроз и выбор мер защиты объектов критической информационной инфраструктуры	Классификация уязвимостей информационной системы, причины возникновения угроз безопасности. Формирование технического задания на создание или модификацию системы защиты объекта критической информационной инфраструктуры. Обсуждение правил выбора средств защиты информации для реализации организационных и технических мер.	2	ПК-1, ПК-3, УК-1, УК-2
	Итого	2	

Согласована на портале № 73593

6 Организационно-распорядительные документы по обеспечению безопасности значимых объектов критической информационной инфраструктуры	Организационно-распорядительные документы по безопасности значимых объектов, определяющие порядок и правила обеспечения безопасности значимых объектов КИИ, определяющие порядок и правила функционирования системы безопасности значимых объектов КИИ	2	ПК-1, ПК-3, УК-1, УК-2
	Итого	2	
Итого за семестр		16	
Итого		16	

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
2 семестр			
1 Понятие критической информационной инфраструктуры	Термины и определения, понятие критической информационной инфраструктуры (КИИ), объекты КИИ	2	ПК-1, ПК-3, УК-1, УК-2
	Итого	2	
2 Правовое обеспечение критической информационной инфраструктуры	Документы, определяющие регулирование отношений в области обеспечения безопасности КИИ. Оценка безопасности КИИ. Государственный контроль в области обеспечения безопасности значимых объектов КИИ. Постановление от 8 февраля 2018 года №127. О порядке категорирования объектов критической информационной инфраструктуры. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»	4	ПК-1, ПК-3, УК-1, УК-2
	Итого	4	
3 Категории объектов критической информационной инфраструктуры	Классификация АСУТП по сфере функционирования, по виду системы, по Приказу ФСТЭК России №31.Критерии значимости объектов КИИ РФ и их значения. Сведения об объекте КИИ и угрозах ИБ. Нарушители ИБ объектов КИИ. Организационные и технические меры, применяемые для обеспечения ИБ КИИ	8	ПК-1, ПК-3, УК-1, УК-2
	Итого	8	

Согласована на портале № 73593

4 Технические и организационные меры безопасности значимых объектов	Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры. Анализ угроз и разработка модели угроз. Проектирование системы безопасности значимого объекта КИИ. Разработка рабочей и эксплуатационной документации. Приказ № 235 от 21.12.2017 г. «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»	6	ПК-1, ПК-3, УК-1, УК-2
	Итого	6	
5 Модели угроз и выбор мер защиты объектов критической информационной инфраструктуры	Классификация уязвимостей информационной системы, причины возникновения угроз безопасности. Формирование технического задания на создание или модификацию системы защиты объекта критической информационной инфраструктуры. Обсуждение правил выбора средств защиты информации для реализации организационных и технических мер.	8	ПК-1, ПК-3, УК-1, УК-2
	Итого	8	
6 Организационно-распорядительные документы по обеспечению безопасности значимых объектов критической информационной инфраструктуры	Организационно-распорядительные документы по безопасности значимых объектов, определяющие порядок и правила обеспечения безопасности значимых объектов КИИ, определяющие порядок и правила функционирования системы безопасности значимых объектов КИИ	4	ПК-1, ПК-3, УК-1, УК-2
	Итого	4	
Итого за семестр		32	
Итого		32	

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

Согласована на портале № 73593

Названия разделов (тем) дисциплины	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
2 семестр				
1 Понятие критической информационной инфраструктуры	Написание конспекта самоподготовки	1	ПК-1, ПК-3, УК-1, УК-2	Конспект самоподготовки
	Подготовка к тестированию	1	ПК-1, ПК-3, УК-1, УК-2	Тестирование
	Подготовка к устному опросу / собеседованию	1	ПК-1, ПК-3, УК-1, УК-2	Устный опрос / собеседование
	Написание отчета по практическому занятию (семинару)	2	ПК-1, ПК-3, УК-1, УК-2	Отчет по практическому занятию (семинару)
	Итого	5		
2 Правовое обеспечение критической информационной инфраструктуры	Написание конспекта самоподготовки	2	ПК-1, ПК-3, УК-1, УК-2	Конспект самоподготовки
	Подготовка к тестированию	3	ПК-1, ПК-3, УК-1, УК-2	Тестирование
	Подготовка к устному опросу / собеседованию	3	ПК-1, ПК-3, УК-1, УК-2	Устный опрос / собеседование
	Написание отчета по практическому занятию (семинару)	4	ПК-1, ПК-3, УК-1, УК-2	Отчет по практическому занятию (семинару)
	Итого	12		
3 Категории объектов критической информационной инфраструктуры	Написание конспекта самоподготовки	1	ПК-1, ПК-3, УК-1, УК-2	Конспект самоподготовки
	Подготовка к тестированию	2	ПК-1, ПК-3, УК-1, УК-2	Тестирование
	Подготовка к устному опросу / собеседованию	1	ПК-1, ПК-3, УК-1, УК-2	Устный опрос / собеседование
	Написание отчета по практическому занятию (семинару)	8	ПК-1, ПК-3, УК-1, УК-2	Отчет по практическому занятию (семинару)
	Итого	12		

Согласована на портале № 73593

4 Технические и организационные меры безопасности значимых объектов	Написание конспекта самоподготовки	2	ПК-1, ПК-3, УК-1, УК-2	Конспект самоподготовки
	Подготовка к тестированию	2	ПК-1, ПК-3, УК-1, УК-2	Тестирование
	Подготовка к устному опросу / собеседованию	2	ПК-1, ПК-3, УК-1, УК-2	Устный опрос / собеседование
	Написание отчета по практическому занятию (семинару)	6	ПК-1, ПК-3, УК-1, УК-2	Отчет по практическому занятию (семинару)
	Итого	12		
5 Модели угроз и выбор мер защиты объектов критической информационной инфраструктуры	Написание конспекта самоподготовки	1	ПК-1, ПК-3, УК-1, УК-2	Конспект самоподготовки
	Подготовка к тестированию	1	ПК-1, ПК-3, УК-1, УК-2	Тестирование
	Подготовка к устному опросу / собеседованию	2	ПК-1, ПК-3, УК-1, УК-2	Устный опрос / собеседование
	Написание отчета по практическому занятию (семинару)	8	ПК-1, ПК-3, УК-1, УК-2	Отчет по практическому занятию (семинару)
	Итого	12		
6 Организационно-распорядительные документы по обеспечению безопасности значимых объектов критической информационной инфраструктуры	Написание конспекта самоподготовки	1	ПК-1, ПК-3, УК-1, УК-2	Конспект самоподготовки
	Подготовка к тестированию	1	ПК-1, ПК-3, УК-1, УК-2	Тестирование
	Подготовка к устному опросу / собеседованию	1	ПК-1, ПК-3, УК-1, УК-2	Устный опрос / собеседование
	Написание отчета по практическому занятию (семинару)	4	ПК-1, ПК-3, УК-1, УК-2	Отчет по практическому занятию (семинару)
	Итого	7		
Итого за семестр		60		
	Подготовка и сдача экзамена	36		Экзамен
Итого		96		

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

Согласована на портале № 73593

занятий

Формируемые компетенции	Виды учебной деятельности			Формы контроля
	Лек. зан.	Прак. зан.	Сам. раб.	
ПК-1	+	+	+	Конспект самоподготовки, Отчет по практическому занятию (семинару), Тестирование, Устный опрос / собеседование, Экзамен
ПК-3	+	+	+	Конспект самоподготовки, Отчет по практическому занятию (семинару), Тестирование, Устный опрос / собеседование, Экзамен
УК-1	+	+	+	Конспект самоподготовки, Отчет по практическому занятию (семинару), Тестирование, Устный опрос / собеседование, Экзамен
УК-2	+	+	+	Конспект самоподготовки, Отчет по практическому занятию (семинару), Тестирование, Устный опрос / собеседование, 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
2 семестр				
Конспект самоподготовки	5	5	5	15
Устный опрос / собеседование	5	5	5	15
Тестирование	0	0	10	10
Отчет по практическому занятию (семинару)	10	10	10	30
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

Согласована на портале № 73593

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. Основы Информационной безопасности / Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А., - Из-во Горячая линия "Телеком", - 2011г., 558 с [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/reader/book/111016.

7.2. Дополнительная литература

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]: — Режим доступа: https://base.garant.ru/71730198/.

2. Постановление Правительства РФ № 162 от 17.02.2018 г. «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]: — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_291398 .

3. Приказ Федеральной службы по техническому и экспортному контролю от 6 декабря 2017 г. N 227 "Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации" (с изменениями и дополнениями) [Электронный ресурс]: — Режим доступа: https://base.garant.ru/71834810/.

7.3. Учебно-методические пособия

7.3.1. Обязательные учебно-методические пособия

1. Давыдова, Е. М. Организация защиты объектов критической информационной инфраструктуры: Учебно-методическое пособие [Электронный ресурс] / Е. М. Давыдова, А. Ю. Якимук. — Томск: ТУСУР, 2022. — 20 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/10003.

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.

Согласована на портале № 73593

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.

8.3. Материально-техническое и программное обеспечение для самостоятельной работы

Для самостоятельной работы используются учебные аудитории (компьютерные классы), расположенные по адресам:

- 634050, Томская область, г. Томск, Ленина проспект, д. 40, 233 ауд.;
- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 209 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Описание имеющегося оборудования:

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

Перечень программного обеспечения:

- 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

Согласована на портале № 73593

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 Понятие критической информационной инфраструктуры	ПК-1, ПК-3, УК-1, УК-2	Конспект самоподготовки	Примерный перечень тем для конспектов самоподготовки
		Устный опрос / собеседование	Примерный перечень вопросов для устного опроса / собеседования
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по практическому занятию (семинару)	Темы практических занятий
2 Правовое обеспечение критической информационной инфраструктуры	ПК-1, ПК-3, УК-1, УК-2	Конспект самоподготовки	Примерный перечень тем для конспектов самоподготовки
		Устный опрос / собеседование	Примерный перечень вопросов для устного опроса / собеседования
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по практическому занятию (семинару)	Темы практических занятий

Согласована на портале № 73593

3 Категории объектов критической информационной инфраструктуры	ПК-1, ПК-3, УК-1, УК-2	Конспект самоподготовки	Примерный перечень тем для конспектов самоподготовки
		Устный опрос / собеседование	Примерный перечень вопросов для устного опроса / собеседования
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по практическому занятию (семинару)	Темы практических занятий
4 Технические и организационные меры безопасности значимых объектов	ПК-1, ПК-3, УК-1, УК-2	Конспект самоподготовки	Примерный перечень тем для конспектов самоподготовки
		Устный опрос / собеседование	Примерный перечень вопросов для устного опроса / собеседования
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по практическому занятию (семинару)	Темы практических занятий
5 Модели угроз и выбор мер защиты объектов критической информационной инфраструктуры	ПК-1, ПК-3, УК-1, УК-2	Конспект самоподготовки	Примерный перечень тем для конспектов самоподготовки
		Устный опрос / собеседование	Примерный перечень вопросов для устного опроса / собеседования
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по практическому занятию (семинару)	Темы практических занятий

Согласована на портале № 73593

6 Организационно-распорядительные документы по обеспечению безопасности значимых объектов критической информационной инфраструктуры	ПК-1, ПК-3, УК-1, УК-2	Конспект самоподготовки	Примерный перечень тем для конспектов самоподготовки
		Устный опрос / собеседование	Примерный перечень вопросов для устного опроса / собеседования
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по практическому занятию (семинару)	Темы практических занятий

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

Согласована на портале № 73593

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. Какое из определений информационных технологий верно
   a) процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
   b) приёмы, способы и методы применения средств вычислительной техники при выполнении функций сбора, хранения, обработки, передачи и использования данных;
   c) ресурсы, необходимые для сбора, обработки, хранения и распространения информации;
   d) все перечисленное.

2. Безопасность информации
   a) состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность;
   b) состояние, при котором невозможно изменить информацию;
   c) состояние, обеспечивающее целостность и защищенность информации;
   d) состояние, при котором злоумышленник не может получить информацию.

3. Безопасность критической информационной инфраструктуры
   a) состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак;
   b) состояние защищенности, при котором обеспечены конфиденциальность, доступность и целостность информации;
   c) состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование;
   d) состояние, обеспечивающее целостность и защищенность информации.

4. Доступ к информации
   a) возможность получения информации и ее использования;
   b) состояние доступности;
   c) возможность проводить сбор, обработку и передачу информации
   d) возможность изменения информации

Согласована на портале № 73593

5. Значимый объект критической информационной инфраструктуры
   a) объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры;
   b) объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости;
   c) информационно-телекоммуникационная сеть;
   d) автоматизированная система управления субъекта критической информационной инфраструктуры.

6. Объект критической информационной инфраструктуры
   a) информационная система, информационно-телекоммуникационная сеть, автоматизированная система управления субъекта критической информационной инфраструктуры;
   b) автоматизированная система управления субъекта критической информационной инфраструктуры;
   c) объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости;
   d) который включен в реестр значимых объектов критической информационной инфраструктуры.

7. Субъекты критической информационной инфраструктуры
   a) государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы;
   b) информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности,
   c) российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей;
   d) все выше перечисленное.

8. Какой закон регулирует отношения в области обеспечения безопасности КИИ РФ в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.
   a) Федеральный закон от 26.07.2017 № 187ФЗ;
   b) Приказ ФСБ России от 19.06.2019 № 281;
   c) Приказ ФСТЭК России от 25 декабря 2017 г. № 239;
   d) Постановление Правительства РФ от 8 февраля 2018 г. № 127.

9. Компьютерный инцидент
   a) любое реальное или предполагаемое событие имеющее отношение к безопасности компьютерной системы или компьютерной сети;
   b) атака на компьютерную систему;
   c) изменение системы безопасности компьютерной сети;
   d) событие изменяющее компьютерную систему.

10. Под … понимается установление соответствия объекта КИИ критериям значимости и показателям их значений, присвоение ему одной из категорий значимости, проверку сведений о результатах ее присвоения.
    a) категорированием;
    b) идентификацией;
    c) установлением значимости;
    d) обеспечением безопасности.

9.1.2. Перечень экзаменационных вопросов

Согласована на портале № 73593

1. Состав технических мер по защите КИИ согласно приказу №239 ФСТЭК
2. Состав организационных мер по защите КИИ согласно приказу №239 ФСТЭК
3. Основные законы в сфере безопасности КИИ
4. Перечислите потенциальные сферы объектов КИИ, кратко охарактеризуйте их
5. Как определяются категории значимости объектов КИИ
6. Основные регуляторы объектов КИИ, их функции
7. Какая информация включается в реестр КИИ
8. Основные требования и последовательность реализаций требований к ИБ объекта КИИ
9. Классификация угроз безопасности объектов КИИ
10. Состав системы безопасности значимых объектов
11. Требования к средствам системы безопасности объектов КИИ

9.1.3. Примерный перечень тем для конспектов самоподготовки

1. Основные законы в сфере безопасности КИИ;
2. Потенциальные сферы объектов КИИ;
3. Категории значимости объектов КИИ.
4. Основные регуляторы объектов КИИ.
5. Состав системы безопасности значимых объектов.

9.1.4. Примерный перечень вопросов для устного опроса / собеседования

1. Классификация АСУТП: требования, параметры, сроки. Категорирование объектов критической информационной инфраструктуры
2. Разработка модели угроз
3. Выбор мер защиты объектов информатизации
4. Сетевые средства ИнфоТеКС для защиты АСУ КИИ
5. Средства VipNet Coordinator IG

9.1.5. Темы практических занятий

1. Термины и определения, понятие критической информационной инфраструктуры (КИИ), объекты КИИ
2. Документы, определяющие регулирование отношений в области обеспечения безопасности КИИ. Оценка безопасности КИИ. Государственный контроль в области обеспечения безопасности значимых объектов КИИ. Постановление от 8 февраля 2018 года №127. О порядке категорирования объектов критической информационной инфраструктуры. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
3. Классификация АСУТП по сфере функционирования, по виду системы, по Приказу ФСТЭК России №31.Критерии значимости объектов КИИ РФ и их значения. Сведения об объекте КИИ и угрозах ИБ. Нарушители ИБ объектов КИИ. Организационные и технические меры, применяемые для обеспечения ИБ КИИ
4. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры. Анализ угроз и разработка модели угроз. Проектирование системы безопасности значимого объекта КИИ. Разработка рабочей и эксплуатационной документации. Приказ № 235 от 21.12.2017 г. «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»
5. Классификация уязвимостей информационной системы, причины возникновения угроз безопасности. Формирование технического задания на создание или модификацию системы защиты объекта критической информационной инфраструктуры. Обсуждение правил выбора средств защиты информации для реализации организационных и технических мер.
6. Организационно-распорядительные документы по безопасности значимых объектов, определяющие порядок и правила обеспечения безопасности значимых объектов КИИ, определяющие порядок и правила функционирования системы безопасности значимых объектов КИИ

Согласована на портале № 73593

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 9.4.

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

Согласована на портале № 73593

доступная форма предоставления заданий оценочных средств, а именно:

– в печатной форме;

– в печатной форме с увеличенным шрифтом;

– в форме электронного документа;

– методом чтения ассистентом задания вслух;

– предоставление задания с использованием сурдоперевода.

Лицам с ограниченными возможностями здоровья и инвалидам увеличивается время на подготовку ответов на контрольные вопросы. Для таких обучающихся предусматривается доступная форма предоставления ответов на задания, а именно:

– письменно на бумаге;

– набор ответов на компьютере;

– набор ответов с использованием услуг ассистента;

– представление ответов устно.

Процедура оценивания результатов обучения лиц с ограниченными возможностями здоровья и инвалидов по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в форме электронного документа;

– в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

– в форме электронного документа;

– в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

– в форме электронного документа;

– в печатной форме.

При необходимости для лиц с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения может проводиться в несколько этапов.

Согласована на портале № 73593

ЛИСТ СОГЛАСОВАНИЯ

Рассмотрена и одобрена на заседании кафедры КИБЭВС
протокол № 1 от «25» 1 2022 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	Е.Ю. Костюченко	Согласовано, c6235dfe-234a-4234-88f9-e1597aac6463

РАЗРАБОТАНО:

Доцент, каф. КИБЭВС	А.Ю. Якимук	Разработано, 4ffdf265-fb78-4863-b293-f03438cb07cc
Доцент, каф. КИБЭВС	Е.М. Давыдова	Разработано, d4acdfdc-18d3-41a1-ac4e-4a426c6b834a

Согласована на портале № 73593