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

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВИАЦИОННОЙ ТРАНСПОРТНОЙ СИСТЕМЫ

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **25.05.03 Техническая эксплуатация транспортного радиооборудования**
Направленность (профиль) / специализация: **Информационно-телекоммуникационные системы на транспорте и их информационная защита**
Форма обучения: **очная**
Факультет: **Радиоконструкторский факультет (РКФ)**
Кафедра: **Кафедра конструирования и производства радиоаппаратуры (КИПР)**
Курс: **5**
Семестр: **9**
Учебный план набора 2021 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	9 семестр	Всего	Единицы
Лекционные занятия	26	26	часов
Практические занятия	26	26	часов
в т.ч. в форме практической подготовки	12	12	часов
Самостоятельная работа	56	56	часов
Общая трудоемкость (включая промежуточную аттестацию)	108	108	часов
	3	3	з.е.

Формы промежуточной аттестация	Семестр
Зачет	9

Томск

1. Общие положения

1.1. Цели дисциплины

1. Сформировать у студентов способность создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов.

1.2. Задачи дисциплины

1. Сформировать у студентов представление об информационной безопасности авиационной транспортной системы.
2. Сформировать представление о типовых уязвимостях в системах киберзащиты.
3. Сформировать опыт использования концепции, стандартов и методов обеспечения кибербезопасности критических инфраструктур авиационной транспортной системы.

2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).
Часть блока дисциплин: Часть, формируемая участниками образовательных отношений.
Модуль дисциплин: Модуль специализации (major).
Индекс дисциплины: Б1.В.02.06.
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		

УК-8. Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	УК-8.1. Знает классификацию и источники чрезвычайных ситуаций природного и техногенного происхождения, причины, признаки и последствия опасностей, способы защиты от чрезвычайных ситуаций, а также принципы организации безопасности труда на предприятии, технические средства защиты людей в условиях чрезвычайной ситуации	Использует на практике классификацию и источники чрезвычайных ситуаций природного и техногенного происхождения, причины, признаки и последствия опасностей, способы защиты от чрезвычайных ситуаций, а также принципы организации безопасности труда на предприятии, технические средства защиты людей в условиях чрезвычайной ситуации
	УК-8.2. Умеет создавать и поддерживать безопасные условия жизнедеятельности, выявлять признаки, причины и условия возникновения чрезвычайных ситуаций, а также оценивать вероятность возникновения потенциальной опасности и принимать меры по ее предупреждению	Создаёт и поддерживает безопасные условия жизнедеятельности, выявляет признаки, причины и условия возникновения чрезвычайных ситуаций, а также оценивает вероятность возникновения потенциальной опасности и принимает меры по ее предупреждению
	УК-8.3. Умеет применять в практической деятельности требования законодательства в области охраны труда, направленные на обеспечение безопасности персонала и населения, в том числе в условиях возникновения чрезвычайных ситуаций природного и техногенного характера	Применяет в практической деятельности требования законодательства в области охраны труда, направленные на обеспечение безопасности персонала и населения, в том числе в условиях возникновения чрезвычайных ситуаций природного и техногенного характера
	УК-8.4. Владеет навыками по применению основных методов защиты при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	Использует на практике навыки по применению основных методов защиты при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов
Общепрофессиональные компетенции		
-	-	-
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 3 зачетных единиц, 108 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
		9 семестр
Контактная аудиторная работа обучающихся с преподавателем, всего	52	52
Лекционные занятия	26	26
Практические занятия	26	26
Самостоятельная работа обучающихся, в т.ч. контактная внеаудиторная работа обучающихся с преподавателем, всего	56	56
Подготовка к зачету	10	10
Подготовка к тестированию	10	10
Подготовка к выступлению (докладу)	36	36
Общая трудоемкость (в часах)	108	108
Общая трудоемкость (в з.е.)	3	3

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
9 семестр					
1 Введение в дисциплину	2	-	2	4	УК-8
2 Киберпреступность и кибертерроризм	4	2	6	12	УК-8
3 Концепции, методы и средства применения кибероружия	2	4	6	12	УК-8
4 Типовые уязвимости в системах киберзащиты	4	4	6	14	УК-8
5 Антивирусные программы и проактивная антивирусная защита	1	4	6	11	УК-8
6 Кибершпионаж, кибербразведка и киберконтрразведка	4	4	6	14	УК-8
7 Особенности обеспечения кибербезопасности конечных точек инфраструктурных систем	2	4	6	12	УК-8
8 Основные направления обеспечения кибербезопасности	2	2	6	10	УК-8
9 Концепции, стандарты и методы обеспечения кибербезопасности критических инфраструктур	3	2	6	11	УК-8
10 Кибербезопасные микросхемы как аппаратная база киберзащищенных АСУТП	2	-	6	8	УК-8

Итого за семестр	26	26	56	108	
Итого	26	26	56	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
9 семестр			
1 Введение в дисциплину	Цели и задачи обеспечения информационной безопасности авиационной транспортной системы. Основные понятия. Характеристика предметной области.	2	УК-8
	Итого	2	
2 Киберпреступность и кибертерроризм	Кибертерроризм. Киберпреступность. О возможности международного соглашения об ограничении распространения кибероружия. Особенности организации и функционирования системы киберзащиты НАТО. Киберпреступления и киберпреступники: классификация, методы "работы" и способы защиты. Этичные хакеры и хактивисты: мифы и реалии.	4	УК-8
	Итого	4	
3 Концепции, методы и средства применения кибероружия	Краткая история развития кибероружия. Методологические принципы классификации кибероружия. Проблемы идентификации исполнителей и заказчиков кибератак.	2	УК-8
	Итого	2	
4 Типовые уязвимости в системах киберзащиты	Уязвимости в микросхемах. Уязвимости в криптографических алгоритмах (стандартах). Преднамеренные уязвимости в шифровальном оборудовании. Уязвимости программного обеспечения информационных систем. Уязвимости бортового оборудования воздушных судов и робототехнических комплексов. Методы выявления программных уязвимостей. Five-Level Problem: пути снижения уязвимостей критических информационных систем.	4	УК-8
	Итого	4	

5 Антивирусные программы и проактивная антивирусная защита	Антивирусные программы. Проактивная антивирусная защита: функции и возможности. Иммунный подход к защите информационных систем.	1	УК-8
	Итого	1	
6 Кибершпионаж, кибер разведка и киберконтрразведка	Классификация, способы и объекты кибершпионажа. Кибер разведка и контрразведка: цели, задачи, методы работы. Структура и основные функции главного управления кибер разведки США. Ежегодные отчеты управления контрразведки США о киберугрозах. Расследование кибератак как высокоприбыльный бизнес и инструмент политической борьбы. Автоматизация процессов кибер разведки с помощью Threat Intelligence Platform. Методологические особенности отбора и подготовки специалистов в области кибер разведки и киберконтрразведки.	4	УК-8
	Итого	4	
7 Особенности обеспечения кибербезопасности конечных точек инфраструктурных систем	Тенденции развития киберугроз, направленных на конечные точки инфраструктурных систем. Тенденция роста бесфайловых (fileless) атак. Рост ущерба от атак на конечные точки. Мировой рынок EDR-решений. Основные платформы Endpoint Detection and Response.	2	УК-8
	Итого	2	
8 Основные направления обеспечения кибербезопасности	Базовые термины и определения кибербезопасности. Редтайминг и блютайминг – «красные», «голубые» и другие «разноцветные» команды. Охота за угрозами как «проактивный метод» киберзащиты. База знаний MITRE ATT&CK. SIEM как важный элемент в архитектуре киберзащиты. Магический квадрант Gartner – что это такое?	2	УК-8
	Итого	2	
9 Концепции, стандарты и методы обеспечения кибербезопасности критических инфраструктур	Тенденции развития и особенности цифровизации промышленных инфраструктур. Оценка рисков безопасности в энергетических системах.	3	УК-8
	Итого	3	

10 Кибербезопасные микросхемы как аппаратная база киберзащищенных АСУТП	Основы проектирования кибербезопасной электронной аппаратуры для АСУТП критических инфраструктур. Использование опыта преоктирования безопасного программного обеспечения при проектировании кибербезопасных микросхем. Современные технологии контроля безопасности в микроэлектронике. Основные алгоритмы (пути) внедрения "зараженных" микросхем в технические объекты вероятного противника.	2	УК-8
	Итого	2	
Итого за семестр		26	
Итого		26	

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
9 семестр			
2 Киберпреступность и кибертерроризм	Киберпреступность и кибертероризм.	2	УК-8
	Итого	2	
3 Концепции, методы и средства применения кибероружия	Концепции, методы и средства применения кибероружия	4	УК-8
	Итого	4	
4 Типовые уязвимости в системах киберзащиты	Типовые уязвимости в системах киберзащиты. Диверсионный анализ.	4	УК-8
	Итого	4	
5 Антивирусные программы и проактивная антивирусная защита	Антивирусные программы и проактивная антивирусная защита	4	УК-8
	Итого	4	
6 Кибершпионаж, киберразведка и киберконтрразведка	Кибершпионаж, киберразведка и киберконтрразведка	4	УК-8
	Итого	4	
7 Особенности обеспечения кибербезопасности конечных точек инфраструктурных систем	Особенности обеспечения кибербезопасности конечных точек инфраструктурных систем	4	УК-8
	Итого	4	
8 Основные направления обеспечения кибербезопасности	Основные направления обеспечения кибербезопасности	2	УК-8
	Итого	2	

9 Концепции, стандарты и методы обеспечения кибербезопасности критических инфраструктур	Концепции, стандарты и методы обеспечения кибербезопасности критических инфраструктур	2	УК-8
	Итого	2	
Итого за семестр		26	
Итого		26	

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
9 семестр				
1 Введение в дисциплину	Подготовка к зачету	1	УК-8	Зачёт
	Подготовка к тестированию	1	УК-8	Тестирование
	Итого	2		
2 Киберпреступность и кибертерроризм	Подготовка к зачету	1	УК-8	Зачёт
	Подготовка к тестированию	1	УК-8	Тестирование
	Подготовка к выступлению (докладу)	4	УК-8	Выступление (доклад) на занятии
	Итого	6		
3 Концепции, методы и средства применения кибероружия	Подготовка к зачету	1	УК-8	Зачёт
	Подготовка к тестированию	1	УК-8	Тестирование
	Подготовка к выступлению (докладу)	4	УК-8	Выступление (доклад) на занятии
	Итого	6		
4 Типовые уязвимости в системах киберзащиты	Подготовка к зачету	1	УК-8	Зачёт
	Подготовка к тестированию	1	УК-8	Тестирование
	Подготовка к выступлению (докладу)	4	УК-8	Выступление (доклад) на занятии
	Итого	6		

5 Антивирусные программы и проактивная антивирусная защита	Подготовка к зачету	1	УК-8	Зачёт
	Подготовка к тестированию	1	УК-8	Тестирование
	Подготовка к выступлению (докладу)	4	УК-8	Выступление (доклад) на занятии
	Итого	6		
6 Кибершпионаж, киберразведка и киберконтрразведка	Подготовка к зачету	1	УК-8	Зачёт
	Подготовка к тестированию	1	УК-8	Тестирование
	Подготовка к выступлению (докладу)	4	УК-8	Выступление (доклад) на занятии
	Итого	6		
7 Особенности обеспечения кибербезопасности конечных точек инфраструктурных систем	Подготовка к зачету	1	УК-8	Зачёт
	Подготовка к тестированию	1	УК-8	Тестирование
	Подготовка к выступлению (докладу)	4	УК-8	Выступление (доклад) на занятии
	Итого	6		
8 Основные направления обеспечения кибербезопасности	Подготовка к зачету	1	УК-8	Зачёт
	Подготовка к тестированию	1	УК-8	Тестирование
	Подготовка к выступлению (докладу)	4	УК-8	Выступление (доклад) на занятии
	Итого	6		
9 Концепции, стандарты и методы обеспечения кибербезопасности критических инфраструктур	Подготовка к зачету	1	УК-8	Зачёт
	Подготовка к тестированию	1	УК-8	Тестирование
	Подготовка к выступлению (докладу)	4	УК-8	Выступление (доклад) на занятии
	Итого	6		
10 Кибербезопасные микросхемы как аппаратная база киберзащищенных АСУТП	Подготовка к зачету	1	УК-8	Зачёт
	Подготовка к тестированию	1	УК-8	Тестирование
	Подготовка к выступлению (докладу)	4	УК-8	Выступление (доклад) на занятии
	Итого	6		
Итого за семестр		56		
Итого		56		

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.	
УК-8	+	+	+	Выступление (доклад) на занятии, Зачёт, Тестирование

6. Рейтинговая система для оценки успеваемости обучающихся

6.1. Балльные оценки для форм контроля

Балльные оценки для форм контроля представлены в таблице 6.1.

Таблица 6.1 – Балльные оценки

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
9 семестр				
Выступление (доклад) на занятии	10	10	10	30
Зачёт	0	0	30	30
Тестирование	10	10	20	40
Итого максимум за период	20	20	60	100
Нарастающим итогом	20	40	100	100

6.2. Пересчет баллов в оценки за текущий контроль

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

Таблица 6.2 – Пересчет баллов в оценки за текущий контроль

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

6.3. Пересчет суммы баллов в традиционную и международную оценку

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

Таблица 6.3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка	Итоговая сумма баллов, учитывает успешно сданный экзамен	Оценка (ECTS)
5 (отлично) (зачтено)	90 – 100	A (отлично)
4 (хорошо) (зачтено)	85 – 89	B (очень хорошо)
	75 – 84	C (хорошо)
	70 – 74	D (удовлетворительно)
3 (удовлетворительно) (зачтено)	65 – 69	
	60 – 64	E (посредственно)
2 (неудовлетворительно) (не зачтено)	Ниже 60 баллов	F (неудовлетворительно)

7. Учебно-методическое и информационное обеспечение дисциплины

7.1. Основная литература

1. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2022. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. [Электронный ресурс]: — Режим доступа: https://urait.ru/bcode/497002.

2. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2022. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. [Электронный ресурс]: — Режим доступа: https://urait.ru/bcode/496741.

3. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2022. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. [Электронный ресурс]: — Режим доступа: https://urait.ru/bcode/498844.

4. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2022. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. [Электронный ресурс]: — Режим доступа: https://urait.ru/bcode/493262.

5. Данилов, А. Н. Основы информационной безопасности : учебное пособие / А. Н. Данилов, С. А. Данилова, А. А. Зорин. — Пермь : ПНИПУ, 2008. — 556 с. — ISBN 978-5-398-00132-7. — Текст : электронный // Лань : электронно-библиотечная система. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/160787.

6. Организация системы управления транспортной безопасностью : учебное пособие / составители Ф. Н. Галиахметов [и др.] ; под редакцией А. В. Дормидонтова. — Ульяновск : УИ ГА, 2019. — 112 с. — Текст : электронный // Лань : электронно-библиотечная система. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/162493.

7. Кучерявый, А. А. Авионика : учебное пособие для вузов / А. А. Кучерявый. — 4-е изд., стер. — Санкт-Петербург : Лань, 2022. — 452 с. — ISBN 978-5-8114-9149-0. — Текст : электронный // Лань : электронно-библиотечная система. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/187688.

7.2. Дополнительная литература

1. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2022. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. [Электронный ресурс]: — Режим доступа: https://urait.ru/bcode/496492.

2. Аполлонский, С. М. Электромагнитная и функциональная безопасности в сложных технических системах : учебное пособие для вузов / С. М. Аполлонский. — Москва : Издательство Юрайт, 2022. — 658 с. — (Высшее образование). — ISBN 978-5-534-14456-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. [Электронный ресурс]: — Режим доступа: https://urait.ru/bcode/496952.

3. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2022. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. [Электронный ресурс]: — Режим доступа: https://urait.ru/bcode/489745.

4. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2022. — 245 с. — (Высшее образование). — ISBN 978-5-9916-7090-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. [Электронный ресурс]: — Режим доступа: https://urait.ru/bcode/490421.

5. Толстобров, А. П. Управление данными : учебное пособие для вузов / А. П. Толстобров. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 272 с. — (Высшее образование). — ISBN 978-5-534-14162-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. [Электронный ресурс]: — Режим доступа: https://urait.ru/bcode/496748.

6. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2022. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. [Электронный ресурс]: — Режим доступа: https://urait.ru/bcode/489242.

7. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2022. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. [Электронный ресурс]: — Режим доступа: https://urait.ru/bcode/491249.

8. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2022. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. [Электронный ресурс]: — Режим доступа: https://urait.ru/bcode/490019.

9. Техническая разведка : учебное пособие / В. В. Смирнов, С. Н. Аникин, М. В. Волков, А. С. Глинкин ; под редакцией В. В. Смирнова. — Санкт-Петербург : БГТУ "Военмех" им. Д.Ф. Устинова, 2019. — 111 с. — ISBN 978-5-907054-61-5. — Текст : электронный // Лань : электронно-библиотечная система. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/157077.

10. Гладких, А. А. Модели, методы и технологии построения перспективных систем обеспечения авиационной безопасности : монография / А. А. Гладких. — Ульяновск : УИ ГА, 2020. — 172 с. — ISBN 975-5-7514-0289-1. — Текст : электронный // Лань : электронно-библиотечная система. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/162495.

11. Караваев, Ю. А. Техническая диагностика : учебное пособие / Ю. А. Караваев, С. А. Ходацкий. — Иркутск : ИФ МГТУ ГА, 2021. — 129 с. — Текст : электронный // Лань : электронно-библиотечная система. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/218282.

7.3. Учебно-методические пособия

7.3.1. Обязательные учебно-методические пособия

1. Рассолов, И. М. Информационное право : учебник и практикум для вузов / И. М. Рассолов. — 6-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 415 с. — (Высшее образование). — ISBN 978-5-534-14327-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. (Рекомендовано для практической и самостоятельной работы). [Электронный ресурс]: — Режим доступа: https://urait.ru/bcode/488767.

2. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2022. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. (Рекомендовано для практической и самостоятельной работы). [Электронный ресурс]: — Режим доступа: https://urait.ru/bcode/489919.

3. Булычев, Г. Г. Программно-аппаратные средства обеспечения информационной безопасности : методические рекомендации / Г. Г. Булычев. — Москва : РТУ МИРЭА, 2020 — Часть 1 — 2020. — 23 с. — Текст : электронный // Лань : электронно-библиотечная система. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/163932.

4. Булычев, Г. Г. Программно-аппаратные средства обеспечения информационной безопасности : методические указания / Г. Г. Булычев. — Москва : РТУ МИРЭА, 2020 — Часть 2 — 2020. — 46 с. — Текст : электронный // Лань : электронно-библиотечная система. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/163812.

5. Организация самостоятельной работы: Учебно-методическое пособие / Д. О. Ноздреватых, Б. Ф. Ноздреватых - 2018. 23 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/7867.

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.

2. Официальный сайт Росавиации Федерального агентства воздушного транспорта Министерства транспорта Российской Федерации (раздел "Информационные системы") https://favt.gov.ru/dejatelnost-is/.

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

Лаборатория ГПО / Лаборатория автоматизированного проектирования: учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа, учебная аудитория для проведения занятий семинарского типа, помещение для курсового проектирования (выполнения курсовых работ), помещение для проведения групповых и индивидуальных консультаций, помещение для проведения текущего контроля и промежуточной аттестации; 634050, Томская область, г. Томск, Ленина проспект, д. 40, 403 ауд.

Описание имеющегося оборудования:

- Мультимедийный проектор TOSHIBA;
- Телевизор-монитор SAMSUNG;
- Магнитно-маркерная доска;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- 7-Zip;
- Acrobat Reader;
- Google Chrome;
- Microsoft Office;
- Microsoft Windows;
- Mozilla Firefox;
- OpenOffice;

Лаборатория прикладного программирования: учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа, учебная аудитория для проведения занятий семинарского типа, помещение для курсового проектирования (выполнения курсовых

работ), помещение для проведения групповых и индивидуальных консультаций, помещение для проведения текущего контроля и промежуточной аттестации; 634050, Томская область, г. Томск, Ленина проспект, д. 40, 302 ауд.

Описание имеющегося оборудования:

- Мультимедиа устройство Hisense H50N5300;
- Магнитно-маркерная доска;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- 7-Zip;
- Acrobat Reader;
- Google Chrome;
- Microsoft Office;
- Microsoft Windows;
- Mozilla Firefox;
- OpenOffice;

8.3. Материально-техническое и программное обеспечение для самостоятельной работы

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

- 634050, Томская область, г. Томск, Ленина проспект, д. 40, 233 ауд.;
- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 201 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Описание имеющегося оборудования:

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

Перечень программного обеспечения:

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

8.4. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья и инвалидов

Освоение дисциплины лицами с ограниченными возможностями здоровья и инвалидами осуществляется с использованием средств обучения общего и специального назначения.

При занятиях с обучающимися с **нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах, мобильной системы преподавания для обучающихся с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой занимаются обучающиеся с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При занятиях с обучающимися с **нарушениями зрения** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для комфортного просмотра.

При занятиях с обучающимися с **нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах, мобильной системы обучения для людей с инвалидностью.

9. Оценочные материалы и методические рекомендации по организации изучения

дисциплины

9.1. Содержание оценочных материалов для текущего контроля и промежуточной аттестации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы, представленные в таблице 9.1.

Таблица 9.1 – Формы контроля и оценочные материалы

Названия разделов (тем) дисциплины	Формируемые компетенции	Формы контроля	Оценочные материалы (ОМ)
1 Введение в дисциплину	УК-8	Зачёт	Перечень вопросов для зачета
		Тестирование	Примерный перечень тестовых заданий
2 Киберпреступность и кибертерроризм	УК-8	Выступление (доклад) на занятии	Примерный перечень тем для выступления (доклада) на занятии
		Зачёт	Перечень вопросов для зачета
		Тестирование	Примерный перечень тестовых заданий
3 Концепции, методы и средства применения кибероружия	УК-8	Выступление (доклад) на занятии	Примерный перечень тем для выступления (доклада) на занятии
		Зачёт	Перечень вопросов для зачета
		Тестирование	Примерный перечень тестовых заданий
4 Типовые уязвимости в системах киберзащиты	УК-8	Выступление (доклад) на занятии	Примерный перечень тем для выступления (доклада) на занятии
		Зачёт	Перечень вопросов для зачета
		Тестирование	Примерный перечень тестовых заданий
5 Антивирусные программы и проактивная антивирусная защита	УК-8	Выступление (доклад) на занятии	Примерный перечень тем для выступления (доклада) на занятии
		Зачёт	Перечень вопросов для зачета
		Тестирование	Примерный перечень тестовых заданий
6 Кибершпионаж, киберразведка и киберконтрразведка	УК-8	Выступление (доклад) на занятии	Примерный перечень тем для выступления (доклада) на занятии
		Зачёт	Перечень вопросов для зачета
		Тестирование	Примерный перечень тестовых заданий

7 Особенности обеспечения кибербезопасности конечных точек инфраструктурных систем	УК-8	Выступление (доклад) на занятии	Примерный перечень тем для выступления (доклада) на занятии
		Зачёт	Перечень вопросов для зачета
		Тестирование	Примерный перечень тестовых заданий
8 Основные направления обеспечения кибербезопасности	УК-8	Выступление (доклад) на занятии	Примерный перечень тем для выступления (доклада) на занятии
		Зачёт	Перечень вопросов для зачета
		Тестирование	Примерный перечень тестовых заданий
9 Концепции, стандарты и методы обеспечения кибербезопасности критических инфраструктур	УК-8	Выступление (доклад) на занятии	Примерный перечень тем для выступления (доклада) на занятии
		Зачёт	Перечень вопросов для зачета
		Тестирование	Примерный перечень тестовых заданий
10 Кибербезопасные микросхемы как аппаратная база киберзащищенных АСУТП	УК-8	Выступление (доклад) на занятии	Примерный перечень тем для выступления (доклада) на занятии
		Зачёт	Перечень вопросов для зачета
		Тестирование	Примерный перечень тестовых заданий

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

Таблица 9.2 – Шкала оценки сформированности планируемых результатов обучения по дисциплине

Оценка	Баллы за ОМ	Формулировка требований к степени сформированности планируемых результатов обучения		
		знать	уметь	владеть
2 (неудовлетворительно)	< 60% от максимальной суммы баллов	отсутствие знаний или фрагментарные знания	отсутствие умений или частично освоенное умение	отсутствие навыков или фрагментарные применение навыков
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. Симметричные шифры являются _____ криптосистемами:
   Выберите один правильный ответ
   а) одноключевыми
   б) многоключевыми
   в) бесключевыми
2. Получение раундовых ключей из основного ключа шифрования называется:
   Выберите один правильный ответ
   а) расписанием использования ключа
   б) процедурой расширения ключа
   в) ключевым пространством
3. Увеличение количества раундов обычно приводит к _____ стойкости алгоритма шифрования:
   Выберите один правильный ответ
   а) повышению
   б) снижению

в) сохранению

4. S-блоком симметричного блочного алгоритма шифрования называется:
   Выберите один правильный ответ
   а) таблица замены группы битов
   б) циклический сдвиг блока битов
   в) таблица перестановки битов в блоке
5. Увеличение количества раундов алгоритма шифрования обычно приводит к _____ его эффективности:
   Выберите один правильный ответ
   а) сохранению
   б) снижению
   в) повышению
6. Элементы шифруемых сообщений в криптографии на эллиптический кривых кодируются:
   Выберите один правильный ответ
   а) точками эллиптической кривой
   б) касательными к эллиптической кривой
   в) целыми числами, взятыми по модулю
7. Аналогом операции возведения числа в степень в криптографии на эллиптических кривых выступает:
   Выберите один правильный ответ
   а) произведение точек
   б) сумма точек
   в) вычисление кратной точки
8. Криптография на эллиптических кривых дает преимущества по сравнению с асимметричными криптосистемами, потому что:
   Выберите один правильный ответ
   а) принципиально не может быть взломана
   б) проще в реализации
   в) обеспечивает эквивалентную защиту при меньшей длине ключа
9. Современные стандарты цифровой подписи являются аналогом криптосистемы _____ на эллиптических кривых.
   Выберите один правильный ответ
   а) RSA
   б) Эль-Гамаля
   в) Диффи—Хеллмана
10. Аналогом операции умножения чисел в криптографии на эллиптических кривых выступает:
    Выберите один правильный ответ
    а) вычисление кратной точки
    б) сумма точек
    в) произведение точек

9.1.2. Перечень вопросов для зачета

1. Киберпреступность и кибертерроризм
2. Концепции, методы и средства применения кибероружия
3. Типовые уязвимости в системах киберзащиты
4. Антивирусные программы и проактивная антивирусная защита
5. Кибершпионаж, киберразведка и киберконтрразведка
6. Особенности обеспечения кибербезопасности конечных точек инфраструктурных систем
7. Основные направления обеспечения кибербезопасности
8. Концепции, стандарты и методы обеспечения кибербезопасности критических инфраструктур
9. Кибербезопасные микросхемы как аппаратная база киберзащищенных АСУТП

9.1.3. Примерный перечень тем для выступления (доклада) на занятии

1. Спуфинг в авиации: угрозы безопасности систем GPS и ADS-B.

2. Анализ информационной уязвимости наземных радиотехнических систем авиационной транспортной системы.
3. Анализ информационной уязвимости бортовых программных систем воздушных судов.
4. Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies.
5. Aviation Cybersecurity and Cyber-Resilience: Assessing Risk in Air Traffic Management.
6. Анализ сценариев киберфизических атак на радиотехнические объекты аэродрома.

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 КИПР
протокол № 6 от «19» 11 2020 г.

СОГЛАСОВАНО:

Должность	Инициалы, фамилия	Подпись
Заведующий выпускающей каф. КИПР	Н.Н. Кривин	Согласовано, 61bb81d6-898a-4d50-b92b-bf79399fcfac
Заведующий обеспечивающей каф. КИПР	Н.Н. Кривин	Согласовано, 61bb81d6-898a-4d50-b92b-bf79399fcfac
Начальник учебного управления	Е.В. Саврук	Согласовано, fa63922b-1fce-4a6a-845d-9ce7670b004c

ЭКСПЕРТЫ:

Доцент, каф. КИПР	Н.Н. Кривин	Согласовано, 61bb81d6-898a-4d50-b92b-bf79399fcfac
Доцент, каф. КИПР	А.А. Чернышев	Согласовано, 72a81577-12a0-4023-8fe9-e3b84d6716fc

РАЗРАБОТАНО:

И.О. заведующего кафедрой, каф. КИПР	Н.Н. Кривин	Разработано, 61bb81d6-898a-4d50-b92b-bf79399fcfac