

Документ подписан электронной подписью
Информация о владельце:
ФИО: Сенченко Павел Васильевич
Должность: Проректор по учебной работе
Дата подписания: 22.09.2023 10:59:28
Уникальный программный ключ:
27e516f4c088deb62ba68945f4406e13fd454355

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ
ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Уровень образования: **высшее образование - специалитет**

Направление подготовки / специальность: **10.05.02 Информационная безопасность телекоммуникационных систем**

Направленность (профиль) / специализация: **Управление безопасностью телекоммуникационных систем и сетей**

Форма обучения: **очная**

Факультет: **Факультет безопасности (ФБ)**

Кафедра: **Кафедра безопасности информационных систем (БИС)**

Курс: **5**

Семестр: **9**

Учебный план набора 2021 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	9 семестр	Всего	Единицы
Лекционные занятия	36	36	часов
Практические занятия	18	18	часов
в т.ч. в форме практической подготовки	6	6	часов
Лабораторные занятия	12	12	часов
в т.ч. в форме практической подготовки	4	4	часов
Самостоятельная работа	78	78	часов
Подготовка и сдача экзамена	36	36	часов
Общая трудоемкость	180	180	часов
(включая промежуточную аттестацию)	5	5	з.е.

Формы промежуточной аттестация	Семестр
Экзамен	9

1. Общие положения

1.1. Цели дисциплины

1. Овладение основными принципами управления уровнем информационной безопасности защищаемых ресурсов организации.

1.2. Задачи дисциплины

1. Получение студентами знаний о структуре и принципах построения политики информационной безопасности организации.

2. Получение студентами умений и навыков по построению моделей угроз и нарушителей и по оценке рисков информационной безопасности в организации.

3. Получение студентами знаний об основных методах контроля обеспечения информационной безопасности в организации.

2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).

Часть блока дисциплин: Обязательная часть.

Модуль дисциплин: Модуль специализации (major).

Индекс дисциплины: Б1.О.05.02.

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
Универсальные компетенции	
УК-10. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	УК-10.1. Знает базовые принципы функционирования экономики и экономического развития общества, источники финансирования профессиональной деятельности, критерии оценки затрат и обоснованности экономических решений
	УК-10.2. Умеет принимать и обосновывать экономические решения в различных областях жизнедеятельности, планировать деятельность с учетом экономически оправданных затрат, направленных на достижение результата
	УК-10.3. Владеет основами финансовой грамотности, а также навыками расчета и оценки экономической целесообразности планируемой деятельности (проекта), ее (его) финансирования из различных источников
Общепрофессиональные компетенции	

ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в процессе функционирования сетей электросвязи в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6.1. Знает основные положения действующих в РФ нормативных правовых актов, нормативных и методических документов по вопросам организации защиты информации ограниченного доступа
	ОПК-6.2. Умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности
	ОПК-6.3. Владеет навыками применения технологий, методов и средств защиты информации ограниченного доступа в процессе функционирования сетей электросвязи
ОПК-9.1. Способен формировать, внедрять и обеспечивать функционирование системы менеджмента информационной безопасности телекоммуникационных систем и сетей	ОПК-9.1.1. Знает стандарты, руководящие и методические документы в области защиты информации в телекоммуникационных системах и сетях
	ОПК-9.1.2. Умеет определять угрозы, реализация которых может привести к нарушению безопасности и корректности функционирования телекоммуникационных систем и сетей, выполнять анализ безопасности и составлять отчеты по результатам проверок защищенности телекоммуникационных систем и сетей
	ОПК-9.1.3. Владеет навыками оценки рисков, связанных с осуществлением угроз безопасности телекоммуникационных систем и сетей
ОПК-15. Способен проводить инструментальный мониторинг качества обслуживания и анализ защищенности информации от несанкционированного доступа в телекоммуникационных системах и сетях в целях управления их функционированием	ОПК-15.1. Знает методики измерения и оценки параметров в телекоммуникационных системах и сетях и типовые средства для инструментальной оценки уровня защищенности телекоммуникационных систем
	ОПК-15.2. Умеет анализировать пропускную способность и предельную нагрузку сети связи, параметры передачи кадров при прохождении по каналам связи, проверять достижимость абонентов сети связи
	ОПК-15.3. Владеет навыками проведения анализа защищенности информации от несанкционированного доступа в телекоммуникационных системах и сетях
Профессиональные компетенции	
-	-

4. Названия разделов (тем) дисциплины

Названия разделов (тем) дисциплины
9 семестр

1 Анализ объекта защиты
2 Внутренние угрозы ИБ
3 Подбор и увольнение сотрудников
4 Текущая работа с персоналом
5 Разграничение доступа и контроль работы сотрудников
6 Управление инцидентами ИБ
7 Системы менеджмента ИБ
8 Свод правил по управлению ИБ
9 Обеспечение защиты информации в экстренных ситуациях