

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Сенченко Павел Васильевич
Должность: Проректор по учебной работе
Дата подписания: 05.11.2023 18:45:00
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

ЗАЩИТА ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В СЕТЯХ И СИСТЕМАХ СВЯЗИ

Уровень образования: **высшее образование - бакалавриат**

Направление подготовки / специальность: **11.03.02 Инфокоммуникационные технологии и системы связи**

Направленность (профиль) / специализация: **Защищенные системы и сети связи**

Форма обучения: **очная**

Факультет: **Радиотехнический факультет (РТФ)**

Кафедра: **Кафедра радиоэлектроники и систем связи (РСС)**

Курс: **3**

Семестр: **6**

Учебный план набора 2023 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	6 семестр	Всего	Единицы
Лекционные занятия	18	18	часов
Практические занятия	16	16	часов
в т.ч. в форме практической подготовки	16	16	часов
Лабораторные занятия	16	16	часов
в т.ч. в форме практической подготовки	16	16	часов
Самостоятельная работа	58	58	часов
Подготовка и сдача экзамена	36	36	часов
Общая трудоемкость	144	144	часов
(включая промежуточную аттестацию)	4	4	з.е.

Формы промежуточной аттестация	Семестр
Экзамен	6

1. Общие положения

1.1. Цели дисциплины

1. Изучение способов защиты информационных процессов в сетях с гибридной физической средой.
2. Изучение возможностей применения стандартных настроек в сетях связи для повышения их защищенности.
3. Работа в компьютерных вычислительных сетях (ВС) с применением программных средств защиты и использования существующих, встроенных в архитектуру ОС, средств связи.

1.2. Задачи дисциплины

1. Изучение способов создания защищенного сетевого соединения, защищенных протоколов связи, защиты от несанкционированного доступа сообщений электронной почты, сетевых ресурсов.
2. Изучение принципов работы брандмауэров, средств предотвращения вторжений, антивирусных программ.
3. Развитие навыков настройки и анализа программных средств защиты, политик безопасности, использования программных отладчиков, сетевых анализаторов.

2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).

Часть блока дисциплин: Часть, формируемая участниками образовательных отношений.

Модуль дисциплин: Модуль направленности (профиля) (major).

Индекс дисциплины: Б1.В.02.09.

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	
-	-
Общепрофессиональные компетенции	
-	-
Профессиональные компетенции	
ПК-1. Способен выполнять математическое и компьютерное моделирование объектов и процессов инфокоммуникационных сетей и систем по типовым методикам для решения профессиональных задач	ПК-1.1. Знает математическое и компьютерное моделирование объектов и процессов инфокоммуникационных сетей и систем по типовым методикам
	ПК-1.2. Умеет выполнять математическое и компьютерное моделирование объектов и процессов инфокоммуникационных сетей и систем по типовым методикам для решения профессиональных задач
	ПК-1.3. Владеет математическим и компьютерным моделированием объектов и процессов инфокоммуникационных сетей и систем по типовым методикам для решения профессиональных задач

4. Названия разделов (тем) дисциплины

Названия разделов (тем) дисциплины

6 семестр

1 Архитектура встроенных средств защиты в ОС. Причины возникновения сбоев в оперативной памяти, общие принципы построения систем защиты (triple functions).
2 Основные понятия, классификация задач, решаемых механизмами идентификации и аутентификации в сетях связи. Идентификация субъекта, понятие протокола идентификации, идентифицирующая информация.
3 Классификация субъектов и объектов доступа. Основные подходы к защите данных от НСД. Абстрактные модели доступа.
4 Виды аудита компьютерных сетей и систем связи, классификация событий.
5 Программно-аппаратные средства шифрования; построение аппаратных компонент криптозащиты данных. Инфраструктура управления открытыми ключами, базовые архитектуры систем управления сертификатами, логическая структура и компоненты PKI.
6 Классификация методов защиты программ со стороны информационных процессов. Методы и средства ограничения доступа к компонентам связи в компьютерных сетях и защиты программ от несанкционированного копирования.
7 Технологии перехвата команд. Системные способы противодействия на основе службы DEP.
8 Протокол компьютерных сетей передачи данных IPSec.
9 Иерархические модели OSI и TCP, их различия. Классы сетей. Служба DNS.
10 Архитектура и возможности ОС. Появление виртуальных машин с ОС, процессы, которые они вызывают. Сетевые сканеры.