

Документ подписан электронной подписью
Информация о владельце:
ФИО: Сенченко Павел Васильевич
Должность: Проректор по учебной работе
Дата подписания: 26.10.2023 11:37:05
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 информации

Уровень образования: **высшее образование - бакалавриат**

Направление подготовки / специальность: **27.03.04 Управление в технических системах**

Направленность (профиль) / специализация: **Управление в робототехнических системах**

Форма обучения: **заочная (в том числе с применением дистанционных образовательных технологий)**

Факультет: **ФДО, Факультет дистанционного обучения**

Кафедра: **КСУП, Кафедра компьютерных систем в управлении и проектировании**

Курс: **5**

Семестр: **9**

Учебный план набора 2020 года

Распределение рабочего времени

№	Виды учебной деятельности	9 семестр	Всего	Единицы
1	Самостоятельная работа под руководством преподавателя	8	8	часов
2	Лабораторные работы	12	12	часов
3	Часы на контрольные работы	2	2	часов
4	Самостоятельная работа	82	82	часов
5	Всего (без экзамена)	104	104	часов
6	Подготовка и сдача зачета	4	4	часов
7	Общая трудоемкость	108	108	часов
			3.0	З.Е.

Контрольные работы: 9 семестр - 1

Зачёт: 9 семестр

Томск

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Изучение комплекса проблем информационной безопасности предприятий и организаций различных типов и направлений деятельности построения, функционирования и совершенствования совокупности правовых, организационных, технических и технологических процессов, обеспечивающих информационную безопасность и формирующих структуру системы защиты ценной и конфиденциальной информации в сфере охраны интеллектуальной собственности и сохранности информационных ресурсов.

1.2. Задачи дисциплины

- Ознакомление студентов с теоретическими основами, основными понятиями и принципами обеспечения информационной безопасности.
- Обучение студентов работе с основными средствами защиты.

2. Место дисциплины в структуре ОПОП

Дисциплина «Защита информации» (Б1.В.02.15) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Базы данных, Вычислительные машины, системы и сети, Информатика, Информационные сети и телекоммуникации, Информационные технологии, Основы электротехники и электроники, Правовые основы профессиональной деятельности.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ОПК-9 способностью использовать навыки работы с компьютером, владеть методами информационных технологий, соблюдать основные требования информационной безопасности ;
- ПК-10 готовностью к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления ;

В результате изучения дисциплины обучающийся должен:

- **знать** базовые концепции и модели информационной безопасности; основы функционирования безопасности информационных систем и задачи информационной безопасности; законодательство по обеспечению информационной безопасности и стандарты в области информационной безопасности
- **уметь** выбирать (разрабатывать) стратегии защиты информационной безопасности различных информационных систем; проводить аудит для отображения уровня соответствия стандартам области информационной безопасности для информационной системы в целом и для ее элементов.
- **владеть** навыками работы с программными и аппаратными средствами обеспечивающими защиту информации в компьютерных системах.

4. Название разделов (тем) дисциплины

Названия разделов дисциплины
9 семестр
1 Правовое обеспечение информационной безопасности
2 Организационное обеспечение информационной безопасности
3 Безопасность операционных систем
4 Безопасность систем баз данных
5 Безопасность вычислительных сетей
6 Криптографические методы защиты информации
7 Технические каналы утечки информации