

Документ подписан электронной подписью
Информация о владельце:
ФИО: Сенченко Павел Васильевич
Должность: Проректор по учебной работе
Дата подписания: 25.10.2023 08:41:15
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: **27.03.03 Системный анализ и управление**

Направленность (профиль) / специализация: **Системный анализ и управление в технических системах**

Форма обучения: **очная**

Факультет: **ФВС, Факультет вычислительных систем**

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

Курс: **4**

Семестр: **7**

Учебный план набора 2020 года

Распределение рабочего времени

№	Виды учебной деятельности	7 семестр	Всего	Единицы
1	Лекции	18	18	часов
2	Лабораторные работы	36	36	часов
3	Всего аудиторных занятий	54	54	часов
4	Самостоятельная работа	54	54	часов
5	Всего (без экзамена)	108	108	часов
6	Общая трудоемкость	108	108	часов
		3.0	3.0	З.Е.

Зачёт: 7 семестр

Томск

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Целью преподавания дисциплины является 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.02.09) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Информатика.

Последующими дисциплинами являются: Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ОПК-7 способностью к освоению новой техники, новых методов и новых технологий ;
- ПК-4 способностью применять методы системного анализа, технологии синтеза и управления для решения прикладных проектно-конструкторских задач ;

В результате изучения дисциплины обучающийся должен:

- **знать** базовые концепции и модели информационной безопасности; основы функционирования безопасности информационных систем задачи информационной безопасности; законодательство по обеспечению информационной безопасности стандарты в области информационной безопасности; методы и средства защиты информационной безопасности направления и методы ведения аналитической работы по выявлению угроз технические процедуры по действиям в нештатной ситуации; методологии оценки рисков и угроз 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 оценивать и выбирать необходимые средства защиты осуществлять мониторинг состояния информационной безопасности объекта обеспечивать противодействие атакам на информационную систему выполнять (контролировать выполнение) требований инструкции по обеспечению информационной безопасности
- **владеть** навыками работы с программными и аппаратными средствами обеспечивающими защиту информации в компьютерных системах

4. Название разделов (тем) дисциплины

Названия разделов дисциплины
7 семестр
1 Базовые понятия в сфере обеспечения информационной безопасности
2 Комплексный подход к обеспечению информационной безопасности
3 Организационно-правовое обеспечение, стандартизация, сертификация и лицензирование в области защиты информации
4 Методы оценки рисков и угроз информационной безопасности

5 Программно-аппаратные, технические и криптографические средства защиты информации
6 Основные принципы, направления и требования обеспечения информационной безопасности организации
7 Концепция и политика информационной безопасности
8 Реализации стратегии обеспечения информационной безопасности
9 Менеджмент информационной безопасности