

Документ подписан электронной подписью  
Информация о владельце:  
ФИО: Сенченко Павел Васильевич  
Должность: Проректор по учебной работе  
Дата подписания: 26.09.2023 12:38:46  
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**

**Безопасность информационных и аналитических систем**

Уровень образования: **высшее образование - специалитет**

Направление подготовки / специальность: **10.05.04 Информационно-аналитические системы безопасности**

Направленность (профиль) / специализация: **Информационная безопасность финансовых и экономических структур**

Форма обучения: **очная**

Факультет: **ФБ, Факультет безопасности**

Кафедра: **БИС, Кафедра безопасности информационных систем**

Курс: **4**

Семестр: **7**

Учебный план набора 2016 года

**Распределение рабочего времени**

№	Виды учебной деятельности	7 семестр	Всего	Единицы
1	Лекции	28	28	часов
2	Практические занятия	18	18	часов
3	Лабораторные работы	16	16	часов
4	Всего аудиторных занятий	62	62	часов
5	Из них в интерактивной форме	18	18	часов
6	Самостоятельная работа	46	46	часов
7	Всего (без экзамена)	108	108	часов
8	Подготовка и сдача экзамена	36	36	часов
9	Общая трудоемкость	144	144	часов
		4.0	4.0	З.Е.

Экзамен: 7 семестр

Томск

## 1. Цели и задачи дисциплины

### 1.1. Цели дисциплины

Раскрыть технологии интеллектуального анализа больших информационных массивов с помощью информационно-аналитических систем.

Дисциплина должна способствовать умению использования информационно-аналитических систем для интеллектуального анализа больших информационных массивов, умению самостоятельно повышать свои знания в области интеллектуального анализа данных, умению применять методы и средства обеспечения информационной безопасности специальных ИАС

### 1.2. Задачи дисциплины

– Задача дисциплины состоит в том, чтобы ознакомить студентов с современными методами и средствами обеспечения информационной безопасности специальных ИАС, с методами оценки эффективности специальных ИАС, в том числе средств обеспечения их информационной безопасности.

## 2. Место дисциплины в структуре ОПОП

Дисциплина «Безопасность информационных и аналитических систем» (Б1.Б.28) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Базы данных и экспертные системы, Информатика, Криптографические методы защиты информации, Математические методы проектирования финансовых систем (групповое проектное обучение - ГПО 1), Методология и организация информационно-аналитической деятельности, Основы информационной безопасности, Прикладная криптография, Проектирование информационно-аналитических систем (групповое проектное обучение - ГПО 2).

Последующими дисциплинами являются: Безопасность программного обеспечения, Моделирование информационно-аналитических систем, Принципы построения, проектирования и эксплуатации информационно-аналитических систем, Распределенные информационно-аналитические системы, Системное программирование, Специальные технологии баз данных и информационных систем, Теоретические основы компьютерной безопасности, Техническая защита информации, Формализованные модели и методы решения аналитических задач.

## 3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ОПК-7 способностью применять методы и средства обеспечения информационной безопасности специальных ИАС;
- ПК-10 способностью осуществлять выбор технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности создаваемых специальных ИАС;
- ПК-13 способностью оценивать эффективность специальных ИАС, в том числе средств обеспечения их информационной безопасности;

В результате изучения дисциплины обучающийся должен:

– **знать** методы и средства обеспечения информационной безопасности специальных ИАС; технологии, инструментальные средства, средства обеспечения информационной безопасности создаваемых специальных ИАС; методы оценки эффективности специальных ИАС, в том числе средств обеспечения их информационной безопасности.

– **уметь** применять методы и средства обеспечения информационной безопасности специальных ИАС; осуществлять выбор технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности создаваемых специальных ИАС; оценивать эффективность специальных ИАС, в том числе средств обеспечения их информационной безопасности.

– **владеть** методами и средствами обеспечения информационной безопасности специальных ИАС; методами оценки эффективности специальных ИАС, в том числе средств обеспечения их информационной безопасности.

#### 4. Название разделов (тем) дисциплины

Названия разделов дисциплины
7 семестр
1 Основные понятия информационно-аналитических систем
2 Методы и средства обеспечения информационной безопасности специальных ИАС
3 Технологии и инструментальные средства информационной безопасности создаваемых специальных ИАС
4 Методы оценки эффективности специальных ИАС, в том числе средств обеспечения их информационной безопасности