**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

# Теоретические основы компьютерной безопасности

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: **5**
Семестр: **10**
Учебный план набора 2016 года

Распределение рабочего времени

| № | Виды учебной деятельности | 10 семестр | Всего | Единицы |
|---|---|---|---|---|
| 1 | Лекции | 28 | 28 | часов |
| 2 | Практические занятия | 36 | 36 | часов |
| 3 | Всего аудиторных занятий | 64 | 64 | часов |
| 4 | Из них в интерактивной форме | 20 | 20 | часов |
| 5 | Самостоятельная работа | 44 | 44 | часов |
| 6 | Всего (без экзамена) | 108 | 108 | часов |
| 7 | Общая трудоемкость | 108 | 108 | часов |
| | | 3.0 | 3.0 | З.Е. |

Зачёт: 10 семестр

Томск

## 1. Цели и задачи дисциплины

### 1.1. Цели дисциплины

обучение студентов комплексному подходу к обеспечению информационной безопасности;

формирование у них представлений об использовании специального математического аппарата для анализа защищенности автоматизированных систем.

### 1.2. Задачи дисциплины

– получить представление об основных угрозах информационной безопасности и методах противодействия данным угрозам;

– изучить основные формальные математические модели, используемые для анализа защищенности автоматизированных систем;

– изучить методологию проектирования и построения защищенных автоматизированных систем.

## 2. Место дисциплины в структуре ОПОП

Дисциплина «Теоретические основы компьютерной безопасности» (Б1.В.ОД.11) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Безопасность операционных систем, Безопасность сетей ЭВМ, Безопасность электронного документооборота, Дискретная математика.

## 3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-5 способностью проводить обоснование и выбор оптимального решения задач в сфере профессиональной деятельности;

– ПК-9 способностью выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах;

– ПК-10 способностью осуществлять выбор технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности создаваемых специальных ИАС;

– ПСК-2.1 способностью проводить комплексный анализ функционирования финансовых и экономических структур государственного или системообразующего уровня с целью выявления угроз (отрицательных тенденций) национальной безопасности Российской Федерации;

В результате изучения дисциплины обучающийся должен:

– **знать** Методологические и технологические основы комплексного обеспечения безопасности автоматизированных систем и их элементов; угрозы нарушения безопасности информационных систем.

– **уметь** выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах; проектировать защищённые автоматизированные системы и их элементы; проводить комплексный анализ информационных систем; проводить обоснование и выбор оптимального решения задач в сфере профессиональной деятельности.

– **владеть** опытом применения технологий, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности создаваемых специальных ИАС.

## 4. Название разделов (тем) дисциплины

| Названия разделов дисциплины |
|---|
| 10 семестр |
| 1 Основные положения теории защиты информации |
| 2 Математическое моделирование в проектировании защищённых телекоммуникационных систем |
| 3 Классификация угроз безопасности информации в телекоммуникационных системах и их элементах |

| |
|---|
| 4 Дискреционное разграничение доступа для обеспечения безопасности телекоммуникационных систем |
| 5 Мандатное разграничение доступа для обеспечения безопасности телекоммуникационных систем |
| 6 Ролевое разграничение доступа для обеспечения безопасности телекоммуникационных систем |
| 7 Изолированная программная среда в проектировании защищённых телекоммуникационных систем и их элементов |
| 8 Защита индивидуальных заданий |