

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Сенченко Павел Васильевич
Должность: Проректор по учебной работе
Дата подписания: 26.09.2023 12:44:32
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

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: **4**

Семестр: **8**

Учебный план набора 2020 года

Распределение рабочего времени

| № | Виды учебной деятельности | 8 семестр | Всего | Единицы |
|---|-----------------------------|-----------|-------|---------|
| 1 | Лекции | 30 | 30 | часов |
| 2 | Практические занятия | 30 | 30 | часов |
| 3 | Всего аудиторных занятий | 60 | 60 | часов |
| 4 | Самостоятельная работа | 48 | 48 | часов |
| 5 | Всего (без экзамена) | 108 | 108 | часов |
| 6 | Подготовка и сдача экзамена | 36 | 36 | часов |
| 7 | Общая трудоемкость | 144 | 144 | часов |
| | | 4.0 | 4.0 | З.Е. |

Экзамен: 8 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.01.01) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Безопасность операционных систем, 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 и методы нарушения безопасности автоматизированных систем
- **уметь** создавать и исследовать модели автоматизированных систем; проектировать защищённые автоматизированные системы и их элементы
- **владеть** опытом применения формальных моделей обеспечения безопасности автоматизированных систем, методами и средствами реализации защищенных автоматизированных систем

4. Название разделов (тем) дисциплины

| Названия разделов дисциплины |
|--|
| 8 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 |

| |
|--|
| 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 |