

Документ подписан электронной подписью  
Информация о владельце:  
ФИО: Сенченко Павел Васильевич  
Должность: Проректор по учебной работе  
Дата подписания: 26.09.2023 12:44:31  
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 операционных 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: **2, 3**

Семестр: **4, 5**

Учебный план набора 2020 года

**Распределение рабочего времени**

№	Виды учебной деятельности	4 семестр	5 семестр	Всего	Единицы
1	Лекции	24	14	38	часов
2	Практические занятия	8	0	8	часов
3	Лабораторные работы	12	28	40	часов
4	Всего аудиторных занятий	44	42	86	часов
5	Самостоятельная работа	64	66	130	часов
6	Всего (без экзамена)	108	108	216	часов
7	Подготовка и сдача экзамена	0	36	36	часов
8	Общая трудоемкость	108	144	252	часов
		3.0	4.0	7.0	З.Е.

Зачёт: 4 семестр

Экзамен: 5 семестр

Томск

## 1. Цели и задачи дисциплины

### 1.1. Цели дисциплины

Целью дисциплины «Безопасность операционных систем» является освоение принципов построения современных операционных систем (ОС) и принципов администрирования подсистемы защиты информации в ОС.

### 1.2. Задачи дисциплины

- Задачи изучения дисциплины – получение студентами:
- – знаний об устройстве и принципах функционирования ОС различной архитектуры;
- – умений и навыков в области администрирования операционных систем;
- – знаний о методах несанкционированного доступа (НСД) к ресурсам ОС;
- – знаний о структуре подсистемы защиты в ОС;
- – навыков использования средств и методов защиты от НСД к ресурсам ОС.

## 2. Место дисциплины в структуре ОПОП

Дисциплина «Безопасность операционных систем» (Б1.Б.05.03) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Безопасность операционных систем, Информатика, Основы информационной безопасности, Языки программирования.

Последующими дисциплинами являются: Безопасность операционных систем, Безопасность сетей ЭВМ, Прикладная криптография.

## 3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ОПК-3 способностью применять в профессиональной деятельности современные средства вычислительной техники и программное обеспечение, достижения информационных технологий для поиска и обработки информации по профилю профессиональной деятельности;
- ПК-10 способностью осуществлять выбор технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности создаваемых специальных ИАС;
- ПК-15 способностью эксплуатировать специальные ИАС и средства обеспечения их информационной безопасности на всех этапах жизненного цикла, а также восстанавливать их работоспособность при внештатных ситуациях;

В результате изучения дисциплины обучающийся должен:

- **знать** – принципы построения и функционирования, примеры реализаций современных операционных систем; – функции операционных систем, основные концепции управления процессорами, памятью, вспомогательной памятью, устройствами; – критерии оценки эффективности и надежности средств защиты операционных систем; – принципы организации и структуру подсистем защиты операционных систем семейств UNIX и Windows.
- **уметь** – использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; – оценивать эффективность и надежность защиты операционных систем; – планировать политику безопасности операционных систем.
- **владеть** – профессиональной терминологией в области информационной безопасности; – навыками работы с операционными системами семейств UNIX и Windows, восстановление операционных систем после сбоев; – навыками установки и настройки операционных систем семейств UNIX и Windows с учетом требований по обеспечению информационной безопасности; – навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности

## 4. Название разделов (тем) дисциплины

Названия разделов дисциплины
------------------------------

4 семестр
1 Общая характеристика ОС
2 Управление памятью
3 Управление устройствами
4 Файловые системы
5 Управление процессами
6 Администрирование ОС
5 семестр
7 Основные механизмы обеспечения безопасности ОС
8 Средства и методы аутентификации в ОС
9 Разграничение доступа к ресурсам ОС
10 Контроль работы подсистемы защиты