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 2016 года

Распределение рабочего времени

№	Виды учебной деятельности	4 семестр	5 семестр	Всего	Единицы
1	Лекции	28	18	46	часов
2	Практические занятия	18	0	18	часов
3	Лабораторные работы	16	36	52	часов
4	Всего аудиторных занятий	62	54	116	часов
5	Из них в интерактивной форме	18	16	34	часов
6	Самостоятельная работа	46	54	100	часов
7	Всего (без экзамена)	108	108	216	часов
8	Подготовка и сдача экзамена	0	36	36	часов
9	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, формирование компетенций применять в профессиональной деятельности современные средства вычислительной техники и программное обеспечение, достижения информационных технологий для поиска и обработки информации по профилю профессиональной деятельности, осуществлять выбор технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности создаваемых специальных ИАС и эксплуатировать специальные ИАС и средства обеспечения их информационной безопасности на всех этапах жизненного цикла, а также восстанавливать их работоспособность при внештатных ситуациях.

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;
- – навыков применения в профессиональной деятельности современных средств вычислительной техники и программного обеспечения, достижений информационных технологий для поиска и обработки информации по профилю профессиональной деятельности;
- – навыков осуществления выборы технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности создаваемых специальных ИАС;
- – навыков эксплуатации специальных ИАС и средств обеспечения их информационной безопасности на всех этапах жизненного цикла, а также восстанавления их работоспособности при внештатных ситуациях.

2. Место дисциплины в структуре ОПОП

Дисциплина «Безопасность операционных систем» (Б1.Б.8) относится к блоку 1 (базовая часть).

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

Последующими дисциплинами являются: Безопасность операционных систем, Безопасность сетей ЭВМ, Прикладная криптография, Системное программирование, Теоретические основы компьютерной безопасности.

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 современных операционных систем и особенности их применения; − основные виды и угрозы безопасности операционных систем; − защитные механиз-

мы и средства обеспечения безопасности операционных систем.

– **уметь** – использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем.

– **владеть** − профессиональной терминологией в области информационной безопасности; − навыками применения в профессиональной деятельности современных средств вычислительной техники и программного обеспечения, достижений информационных технологий для поиска и обработки информации по профилю профессиональной деятельности; − навыками осуществления выбора технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности создаваемых специальных ИАС; − навыками эксплуатации специальных ИАС и средств обеспечения их информационной безопасности на всех этапах жизненного цикла, а также восстановления их работоспособности при внештатных ситуациях.

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
7 Контрольная работа и обсуждение ее результатов
5 семестр
8 Основные механизмы обеспечения безопасности ОС
9 Средства и методы аутентификации в ОС
10 Разграничение доступа к ресурсам ОС
11 Контроль работы подсистемы защиты
12 Контрольная работа и обсуждение ее результатов