АННОТАЦИЯ

Дисциплины

«БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ»

Направление подготовки – 10.05.03 «Информационная безопасность автоматизированных систем»

Квалификация (степень) выпускника – специалист

Специализация – «Информационная безопасность автоматизированных систем на транспорте»

**1. Место дисциплины в структуре основной профессиональной образовательной программы**

Дисциплина «Безопасность операционных систем» (Б1.Б.8) относится к базовой части и является обязательной.

**2. Цель и задачи дисциплины**

Целью изучения дисциплины является расширение и углубление профессиональной подготовки в составе других базовых дисциплин профессионального цикла в соответствии с требованиями, установленными федеральным государственным образовательным стандартом для формирования у выпускника профессиональных компетенций, способствующих решению профессиональных задач в соответствии с видами профессиональной деятельности: научно-исследовательская, проектная, контрольно-аналитическая, организационно-управленческая, эксплуатационная и специализацией «Информационная безопасность автоматизированных систем на транспорте».

Для достижения поставленной цели определены следующие задачи изучения дисциплины:

* подготовка студента по разработанной в университете основной образовательной программе к успешной аттестации планируемых конечных результатов освоения дисциплины;
* подготовка студента к изучению дисциплин, определённых учебным планом в соответствии с указанными компетенциями;
* развитие социально-воспитательного компонента учебного процесса.

При изучении дисциплины решаются следующие конкретные задачи:

* изучение основных принципов построения, назначения и функций операционных систем;
* изучение управления задачами и ресурсами в операционных системах;
* изучение требований к защите операционных систем;
* изучение разграничения доступа в операционных системах;
* изучение аудита в операционных системах.

**3. Перечень планируемых результатов обучения по дисциплине**

Изучение дисциплины направлено на формирование следующих **профессиональных компетенций (ПК)**, соответствующих видам профессиональной деятельности, на которые ориентирована программа специалитета:

*научно-исследовательская деятельность:*

– способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности (ПК-6);

– способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ (ПК-7);

*эксплуатационная деятельность:*

– способностью администрировать подсистему информационной безопасности автоматизированной системы (ПК-26).

В результате освоения 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:

– навыками работы с операционными системами семейств Windows и Unix, восстановления операционных систем после сбоев;

– навыками установки и настройки операционных систем семейств Windows и Unix 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. Содержание и структура дисциплины**

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование раздела дисциплины** | **Содержание раздела** |
|  | Модуль 1 | |
| 1 | Введение в операционные системы | Понятие операционной системы (ОС). Функции ОС. Эволюция ОС. Виды ОС.  Многозадачность. Понятие многозадачности. Виды многозадачности. |
| 2 | Процессы и потоки | Мультипроцессирование: определение, примеры.  Мультипрограммирование (Многозадачность). Планирование. Понятие процесса. Состояние процессов. Виртуальная память.  Создание процессов и потоков. Описатель процесса. Потоки-потомки.  Очереди процессов. Алгоритмы планирования на основе квантования. Алгоритмы планирования на основе приоритетов. Абсолютные и относительные приоритеты. Смешанные алгоритмы планирования.  Планирование в системах реального времени. Виды систем реального времени. Типы запросов в системах реального времени.  Моменты перепланировки. Перепланировка потоков.  Механизм прерываний. Назначение и типы прерываний. Способы прерываний. Программные прерывания. Диспетчеризация и приоритезация прерываний в ОС. Функции централизованного диспетчера прерываний. Обработка прерываний. Процедуры обработки прерываний и текущий процесс.  Синхронизация процессов и потоков. Цели и средства синхронизации. Необходимость синхронизации и гонки. Гонка условий или гонка данных. Критические секции: блокировка. Семафоры. Тупики. Синхронизирующие объекты ОС. Сигналы.  Требования к реализации системных вызовов. Виды системных вызовов. |
| 3 | Управление памятью | Функции ОС по управлению памятью. Типы адресов. Типы виртуальных адресных пространств.  Алгоритмы распределения памяти. Распределение памяти фиксированными разделами. Распределение памяти динамическими разделами. Распределение памяти перемещаемыми разделами.  Свопинг и виртуальная память. Страничное распределение памяти. Сегментное распределение памяти.  Хранение данных. Кэш-память. Типы запоминающих устройств. ПЗУ.  ОЗУ. Иерархия запоминающих устройств.  Кэш-память. Определение. Принцип действия. Схема функционирования. Время доступа. Проблема согласования данных. Способы отображения основной памяти на кэш. Уровни кэш-памяти процессора. |
| 4 | Файловая система | Файл и файловая система. Виды логической организации файловой системы. Монтирование файловых систем  Типы файловых систем. Физическая организация файловой системы и адресация файла. Файловые операции  Организация контроля доступа к файлам. Модели доступа к файлам. Механизм проверки прав доступа. |
| 5 | Концепции распределенной обработки в сетевых ОС | Буферизация в примитивах передачи сообщений. Буферизация в блокирующих примитивах. Буферизация в неблокирующих примитивах. Надежные и ненадежные примитивы: виды и отличия.  Передача сообщений. Механизм Sockets ОС UNIX. Определение. Требования к реализации. Системные вызовы. |
|  | Модуль 2 | |
| 6 | Угрозы безопасности ОС | Классификация угроз информационной безопасности ОС. Основные угрозы безопасности для ОС.  Понятие безопасной ОС. Подходы к организации защиты. Административные меры. Этапы построения защиты. Требования к подсистеме аудита. Политика аудита ОС. |
| 7 | Типовая архитектура подсистемы защиты ОС | Идентификация и аутентификация пользователей. Идентификация и аутентификация на основе многоразового пароля. Идентификация и аутентификация с помощью внешних носителей ключевой информации. Аутентификация на основе цифрового сертификата. Идентификация и аутентификация с помощью биометрических характеристик пользователей.  Управление доступом. Избирательное и полномочное разграничение доступа. Изолированная программная среда.  Аудит безопасности ОС. |
| 8 | Особенности защиты в операционных системах семейства UNIX | Подсистема идентификации и аутентификации Пользовательский идентификатор. Файлы паролей пользователя. Групповой идентификатор.  Подсистема разграничения доступа. Объекты и субъекты доступа. Механизм разграничения доступа к ресурсам. Изменение прав доступа к ресурсам системы.  Подсистема аудита. |
| 9 | Особенности защиты в операционных системах семейства WINDOWS | Подсистема идентификации и аутентификации. Архитектура подсистемы аутентификации. Параметры аутентификации.  Подсистема разграничения доступа. Объекты и субъекты доступа. Атрибуты безопасности пользователя.  Подсистема аудита. |

**5. Объем дисциплины и виды учебной работы**

Объем дисциплины – 8 зачетных единиц (288 час.), в том числе:

лекции – 72 час.

лабораторные работы – 72 час.

практические занятия – 18 час.

самостоятельная работа – 90 час.

контроль – 36 час.

Форма контроля знаний – 5 семестр – экзамен, 6 семестр – зачет, курсовая работа.