МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное учреждение
высшего профессионального образования
"Казанский (Приволжский) федеральный университет"
Институт физики

УТВЕРЖДАЮ
Проректор по образовательной деятельности КФУ
Проф. Таюрский Д.А.
_____ _____20___ г.

подписано электронно-цифровой подписью

Программа дисциплины

Безопасность операционных систем Б1.В.ОД.5

Направление подготовки: 10.03.01 - Информационная безопасность
Профиль подготовки: Безопасность автоматизированных систем
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский

Автор(ы):
Рябченко Е.Ю.

Рецензент(ы):
Шерстюков О.Н.

СОГЛАСОВАНО:
Заведующий(ая) кафедрой: Шерстюков О. Н.
Протокол заседания кафедры No ___ от "____" _____ 201__г
Учебно-методическая комиссия Института физики:
Протокол заседания УМК No ____ от "____" _____ 201__г

Регистрационный No 658618

Казань
2018

Содержание

Программу дисциплины разработал(а)(и) доцент, к.н. Рябченко Е.Ю. Кафедра радиофизики Отделение радиофизики и информационных систем , Eugene.Ryabchenko@kpfu.ru

1. Цели освоения дисциплины

Цели освоения дисциплины - изучение принципов построения современных многопользовательских операционных систем (ОС), включая подсистемы защиты данных и контроля доступа к ресурсам ОС.

2. Место дисциплины в структуре основной образовательной программы высшего профессионального образования

Данная учебная дисциплина включена в раздел " Б1.В.ОД.5 Дисциплины (модули)" основной образовательной программы 10.03.01 Информационная безопасность и относится к обязательным дисциплинам. Осваивается на 3 курсе, 6 семестр.

Дисциплина входит в профессиональный цикл и является обязательной для изучения по основной образовательной программе высшего профессионального образования по специальности: 10.03.01 Информационная безопасность.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля

В результате освоения дисциплины формируются следующие компетенции:

В результате освоения дисциплины студент:

1. должен знать:

основы архитектуры современных операционных систем, применяемых для построения хранилищ данных, сетевых серверов, информационных и вычислительных систем.

2. должен уметь:

устанавливать и конфигурировать современные многопользовательские ОС, анализировать степень защищенности данных и ресурсов, определять политику безопасности и настраивать системы контроля доступа.

3. должен владеть:

навыками администрирования современных ОС и разработки сценариев конфигурирования на наиболее распространенных языках программирования для ОС семейств UNIX и Windows.

4. должен демонстрировать способность и готовность:

контролировать защищенность данных и ресурсов ОС от внешних и внутренних потенциальных нарушений политики безопасности с применением всего спектра средств, предоставляемых данной ОС.

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 4 зачетных(ые) единиц(ы) 144 часа(ов).

Форма промежуточного контроля дисциплины экзамен в 6 семестре.

Суммарно по дисциплине можно получить 100 баллов, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов. Минимальное количество для допуска к зачету 28 баллов.

86 баллов и более - "отлично" (отл.);

71-85 баллов - "хорошо" (хор.);

55-70 баллов - "удовлетворительно" (удов.);

54 балла и менее - "неудовлетворительно" (неуд.).

4.1 Структура и содержание аудиторной работы по дисциплине/ модулю

Тематический план дисциплины/модуля

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Обзор архитектуры операционных систем (ОС). Структура и функции операционной системы.	6	1,2	4	0	0	
2.	Тема 2. Файловая система. Обобщение понятия файла. Устройства как объекты ОС.	6	3,4,5	6	0	0	Тестирование
3.	Тема 3. Многопользовательская среда.	6	6,7,8	6	0	0	Тестирование
4.	Тема 4. Процессы.	6	9,10,11	6	0	0	Тестирование
5.	Тема 5. Средства межпроцессного взаимодействия.	6	12,13	4	0	0	Тестирование
6.	Тема 6. Интерфейс пользователя.	6	14	2	0	0	
7.	Тема 7. Инициализации и функционирование ОС.	6	15,16	4	0	0	
8.	Тема 8. Основные понятия в системах защиты ОС.	6	17,18	4	0	0	
9.	Тема 9. Основы работы в режиме командной строки ОС UNIX.	6	1,2,3	0	0	8	
10.	Тема 10. Дискреционная система контроля доступа.	6	4,5,6	0	0	8	Тестирование
11.	Тема 11. Основы автоматизации задач администрирования ОС.	6	7,8	0	0	8	
12.	Тема 12. Управление процессами и задачами.	6	9,10	0	0	8	

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
13.	Тема 13. Основные средства администрирования учетных записей пользователей и политики безопасности.	6	11,12,13	0	0	4	
.	Тема . Итоговая форма контроля	6		0	0	0	Экзамен
	Итого			36	0	36	

4.2 Содержание дисциплины

Тема 1. Обзор архитектуры операционных систем (ОС). Структура и функции операционной системы.

лекционное занятие (4 часа(ов)):

Структура и функции операционной системы. Аппаратное обеспечение многозадачного режима. Технологии построения ядра. Программный интерфейс. Пользовательская среда.

Тема 2. Файловая система. Обобщение понятия файла. Устройства как объекты ОС.

лекционное занятие (6 часа(ов)):

Организация хранения данных. Физический уровень файловой системы. Операции в файловых системах. Обобщение понятия файла. Структура файловой системы ОС UNIX. Идентификация объектов и ссылки. Устройства как объекты ОС. Символьные и блочные устройства. Идентификация и монтирование дисковых разделов. Виртуальные устройства.

Тема 3. Многопользовательская среда.

лекционное занятие (6 часа(ов)):

Пользователи и группы. Суперпользователь. Учетные записи. Дискреционная система контроля доступа. Дополнительные атрибуты доступа.

Тема 4. Процессы.

лекционное занятие (6 часа(ов)):

Режимы и состояния процесса. Контекст процесса. Создание и завершение процесса. Переменные окружения. Типы процессов. Приоритет процессов.

Тема 5. Средства межпроцессного взаимодействия.

лекционное занятие (4 часа(ов)):

Обзор средств взаимодействия процессов. Механизм сигналов. Стандартные потоки ввода-вывода и каналы. Именованные каналы. Сокеты. Семафоры. Очереди сообщений. Разделяемая память.

Тема 6. Интерфейс пользователя.

лекционное занятие (2 часа(ов)):

Командная оболочка. Алфавитно-цифровые терминалы. Удаленный сетевой доступ. Графическая система X Window. Терминалы типа "тонкий клиент".

Тема 7. Инициализации и функционирование ОС.

лекционное занятие (4 часа(ов)):

Загрузка и инициализация ядра ОС . Процесс init и уровни выполнения. Группы и сеансы процессов.

Тема 8. Основные понятия в системах защиты ОС.

лекционное занятие (4 часа(ов)):

Классификация систем контроля доступа. Списки контроля доступа ACL. Мандатное разграничение доступа.

Тема 9. Основы работы в режиме командной строки ОС UNIX.

лабораторная работа (8 часа(ов)):

Команды файловой системы. Основные пользовательские команды. Перенаправление потоков данных на основе файлов.

Тема 10. Дискреционная система контроля доступа.

лабораторная работа (8 часа(ов)):

Модификация идентификатора владельца процесса. Списки контроля доступа ACL.

Тема 11. Основы автоматизации задач администрирования ОС.

лабораторная работа (8 часа(ов)):

Основы автоматизации задач администрирования ОС. Сценарии оболочки shell. Алгоритмические средства и вызов команд.

Тема 12. Управление процессами и задачами.

лабораторная работа (8 часа(ов)):

Управление процессами и задачами. Средства межпроцессных взаимодействий. Неименованные каналы (pipes). Именованные каналы (FIFO). Сокеты.

Тема 13. Основные средства администрирования учетных записей пользователей и политики безопасности.

лабораторная работа (4 часа(ов)):

Основные средства администрирования учетных записей пользователей и политики безопасности. Аудит системной безопасности. Средства контроля доступа к ресурсам ОС.

4.3 Структура и содержание самостоятельной работы дисциплины (модуля)

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
2.	Тема 2. Файловая система. Обобщение понятия файла. Устройства как объекты ОС.	6	3,4,5	подготовка к тестированию	8	Тестирование
3.	Тема 3. Многопользовательская среда.	6	6,7,8	подготовка к тестированию	4	Тестирование
4.	Тема 4. Процессы.	6	9,10,11	подготовка к тестированию	8	Тестирование
5.	Тема 5. Средства межпроцессного взаимодействия.	6	12,13	подготовка к тестированию	4	Тестирование
10.	Тема 10. Дискреционная система контроля доступа.	6	4,5,6	подготовка к тестированию	12	Тестирование
	Итого				36	

5. Образовательные технологии, включая интерактивные формы обучения

Курс лекций читается на основе мультимедийных технологий, практические занятия проводятся в классе многопользовательского терминального доступа.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

Тема 1. Обзор архитектуры операционных систем (ОС). Структура и функции операционной системы.

Тема 2. Файловая система. Обобщение понятия файла. Устройства как объекты ОС.

Тестирование , примерные вопросы:

1. Выберите неправильное утверждение: 1) владелец-пользователь объекта файловой системы всегда может получить к нему доступ, 2) владелец-пользователь (не root) объекта файловой системы не может изменить владельца данного объекта, 3) владелец-пользователь объекта файловой системы может изменять права доступа к объекту, 4) группа-владелец объекта может иметь меньше прав на объект, чем остальные пользователи, 5) остальные пользователи могут иметь больше прав на объект, чем владелец-пользователь. 2. Какие права доступа нужно установить системному администратору на общесистемный каталог временных файлов (/tmp)? 1) 1777, 2) 0644, 3) 0755, 4) 4777, 5) 4755.

Тема 3. Многопользовательская среда.

Тестирование , примерные вопросы:

1. Какую из перечисленных операций не сможет выполнить пользователь (не root), если он имеет режим доступа --x для каталога /dir? 1) получить краткий перечень объектов каталога без возможности просмотра их атрибутов, 2) удалить информацию из файла /dir/file, если для него имеется режим доступа rw-, 3) получить все атрибуты файла /dir/file, если для него имеется режим доступа ---, 4) получить доступ к объектам каталога /dir/tmp, если для него имеется режим доступа r-x, 5) сделать данный каталог текущим. 2. Укажите команду, влияющую на файл /etc/shadow в ОС UNIX 1) passwd, 2) groupdel, 3) groupadd, 4) groupmod, 5) useradd.

Тема 4. Процессы.

Тестирование , примерные вопросы:

1. В какое состояние переходит процесс во время выполнения системного вызова open()? 1) режим ядра, 2) режим задачи, 3) режим останова, 4) состояние defunct, 5) состояние zombie. 2. Выберите действие, которое не выполняет функция fork(). 1) дочернему процессу возвращается идентификатор родительского процесса, 2) для дочернего процесса копируется контекст родительского процесса, 3) отводится место в таблице процессов под новый процесс, 4) порожденному процессу присваивается уникальный идентификатор, 5) родительскому процессу возвращается идентификатор дочернего процесса.

Тема 5. Средства межпроцессного взаимодействия.

Тестирование , примерные вопросы:

1. Какая из перечисленных характеристик не имеет отношения к потоковому соединению через сокеты? 1) возможность создания неименованного канала обмена данными, 2) буферизация передаваемых данных, 3) возможность применения интерфейса программирования аналогично файлам,\ 4) возможность создания соединения типа ?клиент-сервер?, 5) гарантированная доставка данных. 2. Какой из механизмов IPC позволяет организовать дейтаграммное соединение? 1) сетевой сокет, 2) разделяемая память, 3) семафоры, 4) именованный канал FIFO, 5) очередь сообщений.

Тема 6. Интерфейс пользователя.

Тема 7. Инициализации и функционирование ОС.

Тема 8. Основные понятия в системах защиты ОС.

Тема 9. Основы работы в режиме командной строки ОС UNIX.

Тема 10. Дискреционная система контроля доступа.

Тестирование , примерные вопросы:

1. В каком случае при настройке системы администратор допускает ошибку? 1) chmod 640 /etc/shadow; chmod 666 /etc/passwd, 2) chmod 755 /usr; chmod 755 /usr/bin; chown -R root /usr/bin, 3) mkdir /home; chmod o+x /home; chown root /home, 4) mkdir /tmp; chmod 777 /tmp; chmod o+t /tmp, 5) mkdir /var; chgrp root /var; chmod o-w,u+x /var. 2. Продолжите фразу: бит SGID используется для изменения... 1) правила определения владельца-группы для новых объектов каталога, 2) группы-владельца данного каталога, 3) режима доступа к новым каталогам, создаваемым внутри данного каталога, 4) режима доступа к новым файлам, создаваемым внутри данного каталога, 5) эффективного идентификатора пользователя процесса для исполняемых файлов.

Тема 11. Основы автоматизации задач администрирования ОС.

Тема 12. Управление процессами и задачами.

Тема 13. Основные средства администрирования учетных записей пользователей и политики безопасности.

Тема . Итоговая форма контроля

Примерные вопросы к экзамену:

Билеты к экзамену

БИЛЕТ № 1

1. Избирательное (дискреционное) разграничение доступа. (20 баллов)
2. Функции процесса init и связанные с ним системные файлы. (30 баллов)

БИЛЕТ № 2

1. Символьные и жесткие ссылки: назначение, команды, различия. (20 баллов)
2. Обзор средств взаимодействия процессов с приведением круга решаемых задач. (30 баллов)

БИЛЕТ № 3

1. Символьные и блочные устройства: различия, примеры. (20 баллов)
2. Механизм сигналов. Перечень основных сигналов (из таблицы). (30 баллов)

БИЛЕТ № 4

1. Учетные записи пользователей и связанные с этим системные файлы. (20 баллов)
2. Средства межпроцессного взаимодействия: сокеты. (30 баллов)

БИЛЕТ № 5

1. Функции и структура операционной системы (аппаратные средства, процессы, файловая система, память и пр.). (20 баллов)
2. Графическая система X Window: принцип построения. (30 баллов)

БИЛЕТ № 6

1. Виртуальные устройства (привести примеры). (20 баллов)
2. Стандартные потоки ввода-вывода и неименованные каналы. Привести примеры конвейерной обработки. (30 баллов)

БИЛЕТ № 7

1. Командная оболочка как основной интерфейс пользователя. (20 баллов)
2. Средства межпроцессного взаимодействия: семафоры, очереди сообщений, разделяемая память. (30 баллов)

БИЛЕТ № 8

1. Файловая система: функции и организация хранения данных, физический уровень. (20 баллов)
2. Типы процессов. Приоритет процессов. (30 баллов)

БИЛЕТ № 9

1. Операции в файловых системах. (20 баллов)
3. Идентификация и монтирование дисковых разделов (привести примеры). (30 баллов)

БИЛЕТ № 10

1. Переменные окружения (привести перечень основных переменных). (20 баллов)
2. Загрузка и инициализация ядра ОС. (30 баллов)

БИЛЕТ № 11

1. Эффективный идентификатор пользователя EUID: назначение и варианты использования. (20 баллов)
2. Уровни выполнения. Команды изменения уровня выполнения. (30 баллов)

БИЛЕТ № 12

1. Алфавитно-цифровые терминалы. (20 баллов)
2. Недостатки классической дискреционной системы прав доступа. Система ACL (списки контроля доступа). (30 баллов)

БИЛЕТ № 13

1. Удаленный сетевой доступ. Протоколы. (20 баллов)
2. Классическая дискреционная система прав доступа: режим доступа на основе базовых 9 бит. (30 баллов)

БИЛЕТ № 14

1. Полномочное (мандатное) разграничение доступа. (20 баллов)
2. Классическая дискреционная система прав доступа: дополнительные 3 бита (SetUID, SetGID, Sticky bit). (30 баллов)

БИЛЕТ № 15

1. Концепции построения систем прав доступа в современных ОС (PolicyKit, RBAC). (20 баллов)
2. Средства межпроцессного взаимодействия: именованные каналы. (30 баллов)

БИЛЕТ № 16

1. Терминалы типа "тонкий клиент". (20 баллов)
2. Структура файловой системы ОС UNIX (стандарт FHS). (30 баллов)

БИЛЕТ № 17

1. Основные функции и особенности подсистемы защиты ОС. (20 баллов)
2. Создание и завершение процесса (привести перечень возможных состояний процесса). (30 баллов)

БИЛЕТ № 18

1. Идентификация, аутентификация и авторизация субъектов доступа. Объект и субъект, метод и право доступа. (20 баллов)
2. Аппаратное обеспечение многозадачного режима. Технологии построения ядра ОС (монолитный и микроядерный подходы). (30 баллов)

БИЛЕТ № 19

1. Пользователи и группы. Идентификаторы UID и GID. Суперпользователь root: особенности и привилегии. (20 баллов)
2. Контекст процесса. (30 баллов)

7.1. Основная литература:

1. Рябченко Е.Ю. Архитектура и безопасность операционных систем. Учебное пособие. / Е.Ю. Рябченко. - Казань: Казан. ун-т, 2015. - 157 с. http://dspace.kpfu.ru/xmlui/bitstream/handle/net/20351/06_42_001103.pdf

2. Назаров С.В. Операционные среды, системы и оболочки. Основы структурной и функциональной организации: Учеб. Пособие. - М.: КУДИЦ-ПРЕСС, 2007. - 504 с. http://znanium.com/bookread.php?book=369379

3. Партыка Т.Л., Попов И.И. Операционные системы, среды и оболочки: учебное пособие. - 3-е изд., перераб. и доп. - М.: ФОРУМ, 2010. - 544с. http://znanium.com/bookread.php?book=224882

4. Стахнов А.А. Linux: 4-е изд., перераб. И доп. - СПб.:БХВ-Петербург, 2011. - 752 с. http://znanium.com/bookread.php?book=355362

5. Таненбаум Э. Современные операционные системы. - 3-е изд. - СПб.:Питер, 2015. - 1115 с.

7.2. Дополнительная литература:

1. Колисниченко Д. Н. Серверное применение Linux. ? 3-е изд., перераб и доп. - СПб.: БХВ-Петербург, 2011. - 514 с.: ил. Режим доступа: http://znanium.com/bookread.php?book=355187

7.3. Интернет-ресурсы:

Кузнецов С.Д. Операционная система UNIX. - http://citforum.ru/operating_systems/unix/contents.shtml

Курячий Г.В. Операционная система UNIX. - Интернет университет информационных технологий, 2004. - http://www.intuit.ru/department/os/osunix/

Рябченко Е.Ю. Архитектура операционных систем семейства UNIX. Учебное пособие - http://radiosys.ksu.ru/?p=14

Рябченко Е.Ю. Безопасность ОС. Практический курс. - http://radiosys.ksu.ru/?p=117

Федосеев А. UNIX: учебный курс. - 2006. - http://www.openspin.org/materials/courses/admin/index.html

8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Безопасность операционных систем" предполагает использование следующего материально-технического обеспечения:

Компьютерный класс, представляющий собой рабочее место преподавателя и не менее 15 рабочих мест студентов, включающих компьютерный стол, стул, персональный компьютер, лицензионное программное обеспечение. Каждый компьютер имеет широкополосный доступ в сеть Интернет. Все компьютеры подключены к корпоративной компьютерной сети КФУ и находятся в едином домене.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен студентам. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, УМК, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего профессионального образования (ФГОС ВПО) нового поколения.

Класс многопользовательского терминального доступа, сервер.

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 10.03.01 "Информационная безопасность" и профилю подготовки Безопасность автоматизированных систем .

Автор(ы):
Рябченко Е.Ю. _____
"__" _____ 201 __ г.

Рецензент(ы):
Шерстюков О.Н. _____
"__" _____ 201 __ г.