МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Воронежский государственный технический университет»

УТВЕРЖДАЮ
Декан факультета _____ С.М. Пасмурнов
«31» августа 2017 г.

РАБОЧАЯ ПРОГРАММА
дисциплины

«Безопасность операционных систем»

Специальность 10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Специализация Обеспечение информационной безопасности распределенных информационных систем

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет

Форма обучения очная

Год начала подготовки 2017

Автор программы _____/Разинкин К.А./

Заведующий кафедрой Систем информационной безопасности _____/ А.Г. Остапенко /

Руководитель ОПОП _____/ А.Г. Остапенко /

Воронеж 2017

1.1.Целидисциплины

Обучить студентов принципам построения защиты информации в ОС и анализ

1.2.Задачиосвоениядисциплины

Задачи дисциплины – дать основы принципов построения подсистем защиты в механизмов защиты информации и возможностей по их преодолению.

Дисциплина«Безопасностьоперационныхсистем»относитсякдисциплинамбазов

3.ПЕРЕ

Процессизучениядисциплины«Безопасностьоперационныхсистем»направленна
ОПК-8-способностьюкосвоениюновыхобразцовпрограммных,техническихсред
ПК-22-способностьюучаствоватьвформированииполитикиинформационнойбез

Компетенция	
ОПК-8	Знать организац
	Уметь организов
	Владеть Навыками
ПК-22	Знать содержани понятие бе
	Уметь проводить
	Владеть навыками

Общаятрудоемкостьдисциплины«Безопасностьоперационныхсистем»составля
Распределениетрудоемкостидисциплиныповидамзанятий

очнаяформаобучения

Видыучебнойработы
Аудиторныезанятия (всего)
В томчисле:
Лекции
Лабораторныеработы (ЛР)
Самостоятельнаяработа
Курсовойпроект
Часынаконтроль
Виды промежуточной аттестации - экзамен, зачет с оценкой

Общая трудоемкость: академические часы зач.ед.

5.1Содержаниеразделовдисциплиныираспределениетрудоемкостиповидам

№ п/п	Наименованиетемы	
1	Основные понятия и положения защиты информации в информационно-вычислительных системах	Предмет защиты Основныепринц
2	Угрозы безопасности информации в информационно-вычислительных системах	Анализ угроз ин направления и м
3	Угрозыбезопасности ОС	Классификация
4	Программно-технический уровень информационной безопасности	Основные поня требований к си информации. Ра
5	Требования к защите ОС	Понятие защищ Стандартыбезоп
6	Анализ защищенности современных операционных систем. Встроенныесредствазащиты Windows, Unix	Анализ выполне Анализсуществу

5.2Переченьлабораторныхработ

1. Анализ защищенности операционных систем семейства Windows.
2. Анализ защищенности операционных систем семейства Unix.
3. Изучение защитных механизмов, реализованных в WindowsXP/2003/Vista.
4. Конфигурирование Activedirectory. Настройка групповых политик.
5. Компоненты и структура PKI в Windows.
6. Шифрование файлов в Windows (EFS).
7. Изучение защитных механизмов, реализованных в Unix. PAM.
8. Исследование методов разграничения доступа в ОС Windwos.
9. Исследование методов разграничения доступа в ОС Unix.
10. Исследование методов идентификации и аутентификации в ОС Windows.

Всоответствиисучебнымпланомосвоениедисциплиныпредусматриваетвыполне
Примернаятематикакурсовогопроекта:«Операционные системы семейства Uni

Задачи,решаемыепривыполнениикурсовогопроекта:

1. Изучить характеристику ОС.
2. Определить последовательность ОС.
3. Составить классификацию развития ОС.
4. Проанализировать современные ОС и выявить их недостатки и достоинства.

Курсовойпроектвключатвсебяграфическуючастьирасчетно-пояснительнуюзап

7.ОЦЕНОЧНЫЕМАТЕРИАЛЬ

7.1.Описаниепоказателейикритериевоцениваниякомпетенцийнаразличны

7.1.1Этаптекущегоконтроля

Результатытекущегоконтролязнанийимежсессионнойаттестацииоцениваютсяп
«аттестован»;
«неаттестован».

Компе-тенция	Результатыобучения,характеризующие сформированностькомпетенции
ОПК-8	Знать организацию управления доступом и защиты ресурсов ОС;
	Уметь организовывать управление доступом и защитой ресурсов ОС;
	Владеть Навыками конфигурирования и администрирования операционных
ПК-22	Знать содержание основных понятий по безопасности операционных сис понятие безопасности информационных систем в нормативных до
	Уметь проводить анализ и оценивание механизмов защиты.
	Владеть навыками построения защиты ОС Windows, Unix.

7.1.2Этаппромежуточногоконтролязнаний

Результатыпромежуточногоконтролязнанийоцениваютсяв7,8семестредляочной
«отлично»;
«хорошо»;
«удовлетворительно»;
«неудовлетворительно».

Компе-тенция	Результатыобучения,характеризующие сформированностькомпетенции	
ОПК-8	Знать организацию управления доступом и защиты ресурсов ОС;	Тест
	Уметь организовывать управление доступом и защитой ресурсов ОС;	Решениестанд
	Владеть Навыками конфигурирования и администрирования операционных систем	Решение прик
ПК-22	Знать содержание основных понятий по безопасности операционных систем; понятие безопасности информационных систем в нормативных документах.	Тест
	Уметь проводить анализ и оценивание механизмов защиты.	Решениестанд
	Владеть навыками построения защиты ОС Windows, Unix.	Решение прик

7.2Примерныйпереченьоценочныхсредств(типовыеконтрольныезаданияи

7.2.1Примерныйпереченьзаданийдляподготовкиктестированию

Что такое облачные вычисления?

✓ *вычисления с использованием браузера и web-сервисов, обеспечивающих в*

вычисления, выполняемые на ноутбуке во время полета в облаках

вычисления, выполняемые в момент наибольшего духовного подъема

вычисления с целью определения облачности при прогнозировании погоды

Что такое управляющая программа операционной системы?

подсистема ОС, управляющая работой сети

подсистема ОС, управляющая работой драйверов устройств

подсистема ОС, управляющая повседневной деятельностью пользователя

✓ *подсистема ОС, управляющая исполнением пользовательских программ*

Что такое гибридный процессор?

гибрид процессора и внешнего устройства

процессор, который может выполнять попеременно команды нескольких архи

✓ *процессор, состоящий из многоядерного центрального процессора и мно*

процессор, объединяющий в сеть несколько компьютеров с различными операц

Каковы основные компоненты аппаратуры компьютера?

кард-ридер, USB-порт и адаптер питания

✓ *процессор, память и устройства ввода-вывода*

устройство ввода с перфокарт, печатающее устройство и два больших шкаф

слот для DVD-диска, динамики и система записи

Каковы основные компоненты ноутбука?

принтер и сканер

устройство для записи на магнитную ленту (стример)

DVD-ROM и дисковод для гибких дисков

✓ *порты USB, адаптеры Bluetooth и Wi-Fi*

Какие компьютеры встраиваются в одежду или имплантируются в тело чело

✓ *носимые компьютеры*

кластеры компьютеров

мобильные устройства

суперкомпьютеры

Как организован режим разделения времени в ОС?

машинное время предоставляется пользователям по очереди, по истечении св

оператор машинного зала планирует время и составляет график, в какое врем

✓ *ОС обрабатывает задания, вводимые и управляемые несколькими пользо*

пользователь заранее планирует и рационально использует свое время

В чем причина фрагментации памяти?

невнимательность пользователя

✓ *несовпадение размеров блоков свободной памяти и требуемых размеров*

большое число запросов

ненадежность операционной системы

Что такое монитор (в операционных системах) ?

программа для управления дисплеем

✓ *упрощенный вариант ОС, выполняющий поочередную обработку и пропу*

программа, выполняющая мониторинг работы ОС

программа для управления процессором

Какие действия со своим заданием пользователь может выполнять в диалоге

изменять код программы своего задания

подглядывать в задания других пользователей

✓ *вводить, активизировать, отлаживать задание, визуализировать резул*

увеличивать приоритет своего задания

7.2.2Примерныйпереченьзаданийдлярешениястандартныхзадач

Какой диалект UNIX развивается и распространяется фирмой Oracle / Sun?

IRIX

Digital UNIX

✓ *Solaris*

HP-UX

Как осуществляется управления памятью в режиме мультипрограммировани

память выделяется каждому заданию по частям

в каждый момент в памяти размещается только одно задание

✓ *в памяти хранится одновременно несколько заданий*

выделяется область памяти, куда поочередно загружаются различные задани

Какова основная платформа для облачных вычислений?

Microsoft SQL Server

✓ *Microsoft Windows Azure*

Microsoft Visual Studio

Microsoft BizTalk

Дано: регистрбазы = 100000, регистргранницы = 300000 .Обращение к какому

999999

✓ *300001*

0

500000

Какие основные действия по управлению процессами выполняет ОС?

визуализация образа процесса на дисплее

сопровождение выполнения каждого процесса своим аудиоклипом

✓ *создание, удаление, приостановка, возобновление, синхронизация, взаимо*

откачку процессов на диск

Какие основные действия по управлению оперативной памятью выполняет О

визуализация содержимого памяти на терминале

✓ *выделение памяти требуемого размера, освобождение заданной област*

криптование содержимого заданного участка памяти

Автоматический сброс содержимого памяти на диск в случае сбоя

Что такое атомарная операция?

операция, выполняемая на процессоре IntelAtom

✓ *операция, для которой обеспечивается, что если ее начал выполнять од*

простейшая машинная команда

операция, выполняющаяся один машинный такт
Какая компонента ОС обеспечивает хранение данных во внешней памяти?
система поддержки командного интерпретатора
управление основной памятью
✓ *управление внешней памятью*
управление процессами
Какая команда устанавливает защиту от обращений к Вашей home -директо
chmod 007 home_dir.
✓ *chmod 700 home_dir.*
rm –rfhome_dir.
chmod 000 home_dir.
Как организуется коммуникация между процессами?
по электронной почте
по мобильному телефону
✓ *с помощью передачи сообщений или общей области памяти*
с помощью чата

7.2.3Примерныйпереченьзаданийдлярешенияприкладныхзадач

В каком порядке нумеруются байты в слове при архитектуре bigendian ?
✓ *слева направо (от старших битов слова к младшим)*
в случайном
справа налево (от младших битов слова к старшим)
в произвольном
Что такое executionstub (заглушка для выполнения)?
перезапуск программы
отмена выполнения программы
фиктивная программа, выполняемая вместо настоящей
✓ *ссылка для вызова головной процедуры при запуске программы*
Что такое открытие файла?
считывание его содержимого в основную память
обнуление признаков защиты файла
✓ *считывание его заголовка и одного или нескольких смежных блоков в осн*
предоставление доступа к файлу другим компьютерам локальной сети
Модули каких уровней абстракции разрешается использовать при реализации
✓ *N-1*
Любых
0
N
В чем основная идея принципа микроядра?
✓ *разработка ОС с минимальным возможным числом модулей, выполняем*
разработка ОС, помещающейся в минимальном объеме памяти
разработка ОС, использующей минимальное число ядер многоядерного процес
разработка ОС с минимальным возможным числом функций
Как можно классифицировать процессы, с точки зрения соотношения их испо
✓ *ориентированные на ввод-вывод, ориентированные на вычисления*

активные и ленивые
ресурсоемкие и экономные
выполняющие ввод-вывод и не выполняющие ввод-вывод
Что такое интерактивный процесс?
процесс, ожидающий ответа от пользователя
✓ *процесс, запускаемый с терминала*
приостановленный процесс
процесс, взаимодействующий с другими процессами
Какими операциями осуществляется непосредственная коммуникация процесс
push, pop
call, exit
✓ *send(M, Process), receive(M, Process).*
send(M, Mailbox), receive(M, Mailbox)
Что такое независимый процесс?
✓ *процесс, выполняемый независимо от других процессов*
процесс, выполняемый независимо от ОС
процесс с непредсказуемым поведением
процесс, реализация которого не зависит от целевой платформы
В какой ОС впервые было реализовано понятие процесса, близкое современном
✓ *“Эльбрус”*
MacOS
UNIX
Solaris
Какими способами может быть создан поток в Java ?
✓ *как подкласс класса Thread*
как класс, реализующий интерфеейсRunnable
как поток ядра
как поток Solaris

7.2.4Примерныйпереченьвопросовдляподготовкикзачету

Непредусмотреноучебнымпланом

7.2.5Примерныйпереченьзаданийдлярешенияприкладныхзадач

1) Предмет защиты информации. Основные положения безопасности информацио
2) Угрозы безопасности ОС.Классификация угроз безопасности ОС. Наиболеерас
3) Требования к защите ОС. Понятие защищенной ОС. Подходы к организации за
4) Основные понятия программно-технического уровня информационной безопас
5) Требования к защите компьютерной информации. Классификация требований
6) Общие подходы к построению систем защиты компьютерной информации. Раз
7) Требования к защите ОС. Понятие защищенной ОС. Подходы к организации за
8) Разграничение доступа в ОС. Субъекты, объекты, методы и права доступа. При
   Примерыреализацииразграничениядоступа в современных ОС.
9) Идентификация и аутентификация пользователей ОС. Понятия идентификации
   подбора паролей. Аутентификация на основе внешних носителей ключа, биоме
10) Аудит в ОС. Необходимость аудита. Требования к подсистеме аудита. Пр
11) Системызащитыпрограммногообеспечения.

7.2.6.Методикавыставленияоценкиприпроведениипромежуточнойаттеста

Экзаменпроводитсяпотест-билетам,каждыйизкоторыхсодержит10вопросов ксимальноеколичествонабранныхбаллов–20.

1.Оценка«Неудовлетворительно»ставитсявслучае,еслистудентнабралменее6

2.Оценка«Удовлетворительно»ставитсявслучае,еслистудентнабралот6до10б

3.Оценка«Хорошо»ставитсявслучае,еслистудентнабралот11до15баллов.

4.Оценка«Отлично»ставится,еслистудентнабралот16до20баллов.

7.2.7Паспортоценочныхматериалов

№п/п	Контролируемыеразделы(темы
1	Основные понятия и положения защиты информации в информацион
2	Угрозы безопасности информации в информационно-вычислительны
3	Угрозыбезопасности ОС
4	Программно-технический уровень информационной безопасности
5	Требования к защите ОС
6	Анализ защищенности современных операционных систем. Встроен

7.3.Методическиематериалы,определяющиепроцедурыоцениванияознаний

Тестированиеосуществляется,либоприпомощикомпьютернойсистемытестирова вляетсяоценкасогласнометодикивыставленияоценкиприпроведениипромежуточнойат

Решениестандартныхзадачосуществляется,либоприпомощикомпьютернойсист наторомивыставляетсяоценка,согласнометодикивыставленияоценкиприпроведениип

Решениеприкладныхзадачосуществляется,либоприпомощикомпьютернойсисте наторомивыставляетсяоценка,согласнометодикивыставленияоценкиприпроведениип

Защитакурсовойработы,курсовогопроектаилиотчетаповсемвидампрактикосуще

8.1Переченьучебнойлитературы,необходимойдляосвоениядисциплины

Савинков А.Ю. Управление памятью в современных операционных система государственный технический университет", 2014. - 1 файл. - 30-00.

8.2Переченьинформационныхтехнологий,используемыхприосуществлени
онноймсети«Интернет»,современныхпрофессиональныхбазданныхиинформацио

http://eios.vorstu.ru/
http://www.studentlibrary.ru/
http://znanium.com/
http://ibooks.ru/
http://e.lanbook.com/
http://www.iprbookshop.ru/

- вузовские электронно-библиотечные системы учебной литературы;
-среды разработки на языках C#, C++, Pascal;
- программы для виртуализации систем: VMWareWorkstation, VirtualPC.

9МАТЕРИАЛЬНО-ТЕХНИЧ

Специализированная лекционная аудитория, оснащенная оборудованием для л

10.МЕТОДИЧЕ

Подисциплине«Безопасностьоперационныхсистем»читаютсялекции,проводятс
Основойизучениядисциплиныявляютсялекции,накоторыхизлагаютсянаиболее
Лабораторныеработывыполняютсяналабораторномоборудованиивсоответстви
Методикавыполнениякурсовогопроектаизложенавучебно-методическомпособи
Контрольусвоенияматериаладисциплиныпроизводитсяпроверкойкурсовогопро

Видучебныхзанятий	
Лекция	Написание конспекта лек Проверка терминов, поня ответов в рекомендуемой
Лабораторнаяработа	Лабораторные работы по лабораторных для подгот источники, решить задачи
Самостоятельнаяработа	Самостоятельная работа с - работа с текстами: учебн - выполнение домашних з - работа над темами для са - участие в работе студенч - подготовка к промежуто
Подготовка к промежуточнойаттестации	Готовиться к промежуточ перед зачетом с оценкой,