Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО«Дагестанский государственный технический университет»

РЕКОМЕНДОВАНО
К УТВЕРЖДЕНИЮ:
Декан, председатель совета факультета Компьютерных технологий, вычислительной техники и энергетики
_____ **Ш.А.Юсуфов**
подпись ИОФ
22.11.2018

УТВЕРЖДАЮ:
Проректор по учебной работе, председатель методического совета ДГТУ
_____ **Н.С. Суракатов**
подпись ИОФ
«24» 11 **2018г.**

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина С1.Б.21 Безопасность операционных систем
наименование дисциплины по ООП и код по ФГОС

специальность 10.05.03-«Информационная безопасность автоматизированных систем
шифр и полное наименование направления

специализация «Безопасность открытых информационных систем»

факультет «Компьютерных технологий, вычислительной техники и энергетики»
наименование факультета, где ведется дисциплина

кафедра Информационная безопасность
наименование кафедры, за которой закреплена дисциплина

Квалификация выпускника (степень) Специалист по защите информации
бакалавр (специалист)
Форма обучения очная, курс 2,3 семестр (ы) 4,5
очная, заочная, др.
Всего трудоемкость в зачетных единицах (часах) 4 ЗЕТ (144 ч)
лекции 68 (час); экзамен 5-1ЗЕТ(36 часов)
(семестр)
практические (семинарские) занятия - (час); зачет 4 (семестр)

лабораторные занятия 68(час); самостоятельная работа 116 (час);

курсовой проект (работа, РГР) - (семестр).

Зав. кафедрой ИБ _____ Г.И. Качаева
подпись

Начальник УО _____ Э.В. Магомаева
подпись

Программа составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.03- «Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем»

Программа одобрена на заседании выпускающей кафедры от 19.11 2018 года, протокол № 3

Зав. выпускающей кафедрой по специализации «Безопасность открытых информационных систем»

Г.И. Качаева

ОДОБРЕНО:

Методической комиссией по укрупненным группам специальностей и направлению подготовки

10.00.00- «Информационная безопасность»

Председатель МК

подпись В.Б. Мелехин ИОФ

«20» 11 2018г.

АВТОР (Ы) ПРОГРАММЫ:

Качаева Г.И., к.э.н., ст. преп. каф. ИБ

ИОФ, уч. степень, ученое звание, подпись

2

1. Цели и задачи освоения дисциплины «Безопасность операционных систем»

Целидисциплины

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

Задачи дисциплины

- Задачи изучения дисциплины – получениестудентами:
- – знаний об устройстве и принципах функционирования ОС различнойархитектуры;
- – умений и навыков в области администрирования операционныхсистем;
- – знаний о методах несанкционированного доступа (НСД) к ресурсамОС;
- – знаний о структуре подсистемы защиты вОС;
- – навыков использования средств и методов защиты от НСД к ресурсамОС.

2. Место дисциплины «Безопасность операционных систем» в структуре ООП бакалавриата

Дисциплина «Безопасность операционных систем»относится к базовой части.Предшествующими дисциплинами,формирующиминачальныезнания,являютсяследующие дисциплины: Информатика, Организация ЭВМ и вычислительных систем, Основы информационной безопасности, Языки программирования.

Последующими дисциплинами являются: Программно- аппаратные средства обеспечения информационной безопасности.

3. Требования к результатам освоениядисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ПК-3 способностью проводить анализ защищенности автоматизированныхсистем;
- ПК-14 способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации;
- ПК-17 способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечкиинформации;
- ПК-24 способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности;
- ПК-27 способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы/

В результате изучения дисциплины студент 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 иWindows.
- **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. Структура и содержание дисциплины «Безопасность операционных систем»

4.1.Содержание дисциплины

№ п/п	Раздел дисциплины Тема лекции и вопросы	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего* контроля успеваемости (по срокам текущих аттестаций в семестре)
				ЛК	ПЗ	ЛР	СР	
1	**Лекция № 1** **Тема: «Общая характеристика ОС»** История развития ОС. Назначение и функции ОС и ее подсистем. Системы разделения времени, пакетной обработки, реального времени.	4	1	2			4	Вх. контр.
2	**Лекция № 2** **Тема: «Основные понятия и положения защиты информации в информационно-вычислительных системах».** Предмет защиты информации. Основные положения безопасности информационных систем. Основные принципы обеспечения информационной безопасности в информационных системах.		2	2			4	Контрольная работа № 1
3	**Лекция № 3** **Тема: «Угрозы безопасности информации в информационно--вычислительных системах»** Анализ угроз информационной безопасности. Методы обеспечения информационной безопасности. Классификация злоумышленников		3	2			4	
4	**Лекция № 4** **Тема: «Управление памятью».** Методы распределения памяти. Защита памяти.		4	2		2	4	
5	**Лекция № 5** **Тема: «Основные направления и методы реализации угроз информационной безопасности»** Угрозы безопасности ОС. Классификация угроз безопасности ОС. Наиболее распространенные угрозы		5	2		4	6	
6	**Лекции № 6** **Тема: «Управление устройствами».** Прерывания в ОС. Структура и функции подсистемы управления устройствами ввода-вывода.		6	2		4	4	
7	**Лекции № 7** **Тема: «Программно-технический уровень информационной безопасности»** Основные понятия программно- технического уровня информационной безопасности. Требования к защите компьютерной информации. Классификация требований к системам защиты.		7	2			6	
8	**Лекция № 8** **Тема: «Файловые системы»** Физическая организация файловых систем. Логическая организация файловых систем.		8	2		4	4	
9	**Лекция № 9** **Тема: «Формализованные требования к защите информации от НСД»** Общие подходы к построению систем защиты компьютерной информации. Различия требований и основополагающих механизмов защиты от НСД.		9	2			6	Контрольная работа № 2
10	**Лекция № 10** **Тема: «Требования к защите ОС»** Понятие защищенной ОС. Подходы к организации защиты ОС и их недостатки. Этапы построения защиты.		10	2		4	4	

	Административные меры защиты. Стандарты безопасности ОС							
11	**Лекция № 11** **Тема: «Управление процессами».** Типы программ, работа со службами. Организация динамических и статических вызовов.		11	2			4	
12	**Лекция № 12** **Тема: «Управление процессами».** Процессы и потоки. Дескрипторы процесса и потока. Сохранение и восстановление процессов и потоков. Планирование потоков. Синхронизация процессов.		12	2		4	6	
13	**Лекция № 13** **Тема: «Анализ выполнения современными ОС формализованных требований к защите информации от НСД»** Анализ существующей статистики угроз для современных универсальных ОС		13	2			4	
14	**Лекция № 14** **Тема: «Управление процессами».** Тупиковые ситуации. Наследование ресурсов. Межпроцессное взаимодействие.		14	2		4	6	
15	**Лекция №15** **Тема: «Субъекты, объекты, методы и права доступа»** Привилегии субъектов доступа. Избирательное и полномочное разграничение доступа, изолированная программная среда. Примеры реализации разграничения доступа в современных ОС.		15	2		4	4	Контрольная работа №3
16	**Лекция №16** **Тема: «Администрирование ОС».** Задачи и принципы сопровождения системного программного обеспечения. Настройка, измерение производительности и модификация ОС.		16	2		4	6	
17	**Лекции № 17** **Тема: «Контрольная работа и обсуждение ее результатов»** Обсуждение результатов контрольной работы.		17	2				
Итого за 4 семестр				**34**		**34**	76	**зачет**
18	**Лекция №1** **Тема: «Понятия идентификации и аутентификации пользователей»** Аутентификация на основе паролей, методы подбора паролей, средства и методы повышения защищенности ОС от подбора паролей. Аутентификация на основе внешних носителей ключа, биометрических характеристик пользователя. Примеры реализации идентификации и аутентификации в современных ОС.		1	2			4	Вх. контр.
19	**Лекция №2** **Тема: «POSIX-совместимые операционные системы»** Особенности архитектуры. История развития. Общая характеристика языка командного интерпретатора POSIX-совместимых ОС.		2	2		4	2	
20	**Лекция №3** **Тема: «Переменные языка»** Переменные языка командного интерпретатора POSIX-совместимых ОС и их использование. Встроенные переменные.		3	2			2	Контрольная работа №4
21	**Лекция №4** **Тема: «Средства и методы аутентификации в ОС».** Типовые угрозы безопасности ресурсов ОС. Требования к безопасности ОС. Основные группы механизмов защиты ресурсов ОС.Аутентификация на основе пароля. Аутентификация с использованием физического объекта.		4	2		4	4	

	Биометрические методы аутентификации. Многофакторная аутентификация. Технология SSO.							
22	**Лекция № 5** **Тема: «Управление»** Управление порядком выполнения действий в языке командного интерпретатора POSIX-совместимых ОС. Команды для работы с файлами, каталогами, процессами, перенаправление ввода-вывода		5	2			2	
23	**Лекция № 6** **Тема: «Отладка сценариев»** Назначение и функции систем выполнения сценариев Windows. Объектные модели и языки систем выполнения сценариев ОС Windows.		6	2		4	2	
24	**Лекция № 7** **Тема: «Разграничение доступа к ресурсам ОС».** Классификация субъектов и объектов доступа. Права доступа. Методы разграничения доступа. Разграничение доступа к файловым объектам.Методы разграничения доступа. Разграничение доступа к файловым объектам.		7	2			4	
25	**Лекция № 8** **Тема: «Разграничение доступа к ресурсам ОС».** Разграничение доступа к устройствам. Ограничения на запуск программного обеспечения. Разграничение доступа к устройствам. Ограничения на запуск программного обеспечения.		8	2		4	2	
26	**Лекция № 9** **Тема: «Классификация угроз безопасности ОС»** Наиболее распространенные угрозы. Понятие защищенной ОС.		9	2			2	
27	**Лекция№10** **Тема «Подходы к организации защиты»** Этапы построения защиты. Административные меры защиты.		10	2		2	2	
28	**Лекция№11** **Тема «Контроль работы подсистемы защиты».** Организация и использование средств аудита. Контроль и восстановление целостности подсистемы защиты и ее параметров. Организация и использование средств аудита. Контроль и восстановление целостности подсистемы защиты и ее параметров. Контроль и восстановление целостности подсистемы защиты и ее параметров.		11	2			2	Контрольная работа №5
29	**Лекция№12** **Тема «Стандарты безопасности ОС»** Виртуальные машины. Изоляция процессов и пользователей. Политики безопасности в ОС Windows		12	2		4	2	
30	**Лекция№13** **Тема «Контроль работы подсистемы защиты».** Контроль и восстановление целостности подсистемы защиты и ее параметров. Управление безопасностью ОС. Контроль и восстановление целостности подсистемы защиты и ее параметров. Управление безопасностью ОС.		13	2			2	
31	**Лекция№14** **Тема «Аудит».** Необходимость аудита. Требования к подсистеме аудита. Централизованный аудит. Штатный аудит в ОС Windows. Реализации аудита в современных ОС		14	2		4	2	
32	**Лекция№15** **Тема «Администрирование ОС».** Навыки 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.		15	2		4	2	Контрольная работа №6

33	**Лекция№16** **Тема «Администрирование ОС».** Восстановление операционных систем после сбоев; навыками установки и настройки операционных систем семейств UNIX и Windows с учетом требований по обеспечению информационной безопасности.		16	2		4	4	
34	**Лекция№17** Тема «Контрольная работа и обсуждение ее результатов» Обсуждение результатов контрольной работы.		17	2				
Итого за 5 семестр				**34**		**34**	**40**	**Экзамен (1 зет - 36часов)**
Итого по дисциплине				**68**		68	**116**	

1.2. Содержание лабораторных занятий

№ п/п	№ лекции из рабочей программы	Наименование лабораторного занятия	Количество часов	Рекомендуемая литература и методические разработки (№ источника из списка литературы)
1	2	3	4	5
1	1-3	Анализ защищенности операционных систем Windows и Unix	6	1-10
2	4-5	Изучение защитных механизмов, ре&чизованных в Windows	4	1,2,5,10
3	6-7	Конфигурирование Active directory. Настройка групповых политик		2,3,5,9,10
4	8-9	Компоненты и структура PKI в Windows	4	1,3,6,7,10
5	10-11	Шифрование файлов в Windows (EFS)	4	2,10
6	12-13	Исследование методов разграничения доступа в ОС Windows и Unix	4	2,3,5,9,10
7	14-15	Исследование методов идентификации и аутентификации в ОС Windows и Unix	4	1,3,6,7,10
8	16,17	Настройка системы аудита в Windows и Unix	4	2,10
Итого за 4 семестр			34	
9	1,2	Изучение средств защиты сетевого взаимодействия Windows. Конфигурирование средств защиты каналов средствами Windows, Windows Firewall. Виртуальные частные сети, протоколы L2TP и PPTP	4	1,3,4,7,8.10
10	3,4	Применение карантина для обеспечения безопасности мобильных пользователей на Windows	4	2,4,6,8,10
11	5-,6	Настройки зон безопасности. Централизованная настройка приложений через групповые политики. Защита от неправомерных изменений конфигурации рабочих станций и серверов, от использования неучтенных программ	4	1,2,5,10
12	7,8	Анализ параметров безопасности и конфигурирование безопасности систем под управлением Windows. Применение шаблонов безопасности для защиты рабочих станций пользователей под управлением Windows	4	2,3,5,9,10
13	9,10	Защита серверов под управлением Windows 2003 с использованием Security configuration wizard	4	1,3,6,7,10
14	11,12	Анализ параметров безопасности с использованием Security Configuration and Analysis	4	1,2,5,10
15	13,14	Защита Active Directory	4	2,3,5,9,10
16	15-17	Защита DNS, FTP, DHCP	6	1,3,6,7,10
Итого за 5 семестр			**34**	
Итого по дисциплине			**68**	

4.3 Тематика для самостоятельной работы студента

№ п/п	Тематика по содержанию дисциплины, выделенная для самостоятельного изучения	Количество часов из содержания дисциплины	Рекомендуемая литература и источники информации	Формы контроля СРС
1	2	3	4	5
1	Общая характеристика ОС	8	1-10	
2	Управление памятью	14	1-10	Доклад
3	Управление устройствами	10	1,2,5,10	Реферат
4	Файловые системы	14	2,3,5,9,10	Доклад
5	Управление процессами	20	1,3,6,7,10	Доклад
6	Администрирование ОС	10	2,10	Доклад
7	Основные механизмы обеспечения безопасности ОС	6	1,3,4,7,8.10	Реферат
8	Средства и методы аутентификации в ОС	6	2,4,6,8,10	Доклад
9	Разграничение доступа к ресурсам ОС	12	1,2,5,10	Реферат
10	Контроль работы подсистемы защиты	10	2,3,5,9,10	Реферат
	Администрирование ОС	6	1,3,6,7,10	Доклад
Итого		116		

5.Образовательные технологии

В рамках курса «экономическая теория» уделяется особое внимание установлению межпредметных связей, демонстрации возможности применения полученных знаний в практической деятельности.

В лекционных занятиях используются следующие инновационные методы:

групповая форма обучения - форма обучения, позволяющая обучающимся эффективно взаимодействовать в микрогруппах при формировании и закреплении знаний;

компетентностный подход к оценке знаний - это подход, акцентирующий внимание на результатах образования, причем в качестве результата рассматривается не сумма усвоенной информации, а способность человека действовать в различных проблемных ситуациях;

личностно-ориентированное обучение-это такое обучение, где во где во главу угла ставится личность обучаемого, ее самобытность, самоценность, субъективный опыт каждого сначала раскрывается, а затем согласовывается с содержанием образования;

междисциплинарный подход- подход к обучению, позволяющий научить студентов самостоятельно «добывать» знания из разных областей, группировать их и концентрировать в контексте конкретной решаемой задачи;

развивающее обучение- ориентация учебного процесса на потенциальные возможности человека и их реализацию. В концепции развивающего обучения учащийся рассматривается не как объект обучающих воздействий учителя, а как самоизменяющийся субъект учения.

В процессе выполнения практических занятий используются следующие методы:

исследовательский метод обучения – метод обучения, обеспечивающий возможность организации поисковой деятельности обучаемых по решению новых для них проблем,

процессе которой осуществляется овладение обучаемыми методами научными познания и развитие творческой деятельности;

метод рейтинга - определение оценки деятельности личности или события. В последние годы начинает использоваться как метод контроля и оценки в учебно-воспитательном процессе;

проблемно-ориентированный подход- подход к обучению позволяющий сфокусировать внимание студентов на анализе и разрешении, какой либо конкретной проблемной ситуации, что становится отправной точкой в процессе обучения.

Удельный вес занятий, проводимых в интерактивной форме, составляют не менее 20% аудиторных занятий (25 ч.).

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

Вопросы для входной контрольной работы

1. Дать определение и характеристику основных режимов работы, дисциплин и режимов обслуживания заявок в вычислительных системах.
2. Дать определение и характеристику классов программных средств.
3. Изложить классификацию ОС.
4. Охарактеризовать основные принципы построения ОС.
5. Перечислить виды интерфейсов ОС. Охарактеризовать пакетную технологию как интерфейс. Дать описание интерфейса командной строки.
6. Дать описание графических интерфейсов. В каких ОС они применяются?
7. Охарактеризовать речевую технологию как интерфейс.
8. Охарактеризовать биометрическую технологию как интерфейс.
9. Охарактеризовать семантический интерфейс.

Контрольные работы по проверке текущих знаний студентов

Контрольная работа №1

1. Основные понятия и положения защиты информации в информационно-вычислительных системах.
2. Предмет защиты информации.
3. Основные положения безопасности информационных систем.
4. Основные принципы обеспечения информационной безопасности в информационных системах
5. Угрозы безопасности информации в информационно-вычислительных системах
6. Анализ угроз информационной безопасности.

Контрольная работа №2

1. Методы обеспечения информационной безопасности.
2. Классификация злоумышленников
3. Основные направления и методы реализации угроз информационной безопасности.
4. Угрозы безопасности ОС.
5. Классификация угроз безопасности ОС. Наиболее распространенные угрозы
6. Программно-технический уровень информационной безопасности
7. Основные понятия программно-технического уровня информационной безопасности.
8. Требования к защите компьютерной информации. Классификация требований к системам защиты.
9. Формализованные требования к защите информации от НСД.

Контрольная работа №3

1. Общие подходы к построению систем защиты компьютерной информации.
2. Различия требований и основополагающих механизмов защиты от НСД
3. Требования к защите ОС.
4. Понятие защищенной ОС.
5. Подходы к организации защиты ОС и их недостатки.
6. Этапы построения защиты. Административные меры защиты.
7. Стандарты безопасности ОС
8. Анализ выполнения современными ОС формализованных требований к защите информации от НСД.
9. Анализ существующей статистики угроз для современных универсальных ОС
10. Субъекты, объекты, методы и права доступа. Привилегии субъектов доступа.

Вопросы к зачету по дисциплине «Безопасность операционных систем»

1. Основные понятия и положения защиты информации в информационно-вычислительных системах.
2. Основные положения безопасности информационных систем.
3. Угрозы безопасности информации в информационно-вычислительных системах
4. Анализ угроз информационной безопасности.
10. Методы обеспечения информационной безопасности.
11. Угрозы безопасности ОС.
12. Классификация угроз безопасности ОС. Наиболее распространенные угрозы
13. Программно-технический уровень информационной безопасности
14. Основные понятия программно-технического уровня информационной безопасности.
11. Различия требований и основополагающих механизмов защиты от НСД
12. Требования к защите ОС.
13. Понятие защищенной ОС.
14. Подходы к организации защиты ОС и их недостатки.
15. Этапы построения защиты. Административные меры защиты.
16. Стандарты безопасности ОС
17. Анализ существующей статистики угроз для современных универсальных ОС

Вопросы для входной контрольной работы

1. Основные положения безопасности информационных систем.
2. Анализ угроз информационной безопасности.
3. Угрозы безопасности ОС.
4. Классификация угроз безопасности ОС. Наиболее распространенные угрозы
5. Основные понятия программно-технического уровня информационной безопасности.
6. Различия требований и основополагающих механизмов защиты от НСД
7. Требования к защите ОС.
8. Понятие защищенной ОС.
9. Подходы к организации защиты ОС и их недостатки.
10. Этапы построения защиты. Административные меры защиты.
11. Стандарты безопасности ОС

Контрольная работа №4

1. Избирательное и полномочное разграничение доступа, изолированная программная среда. Примеры реализации разграничения доступа в современных ОС

2. Понятия идентификации и аутентификации пользователей.
3. Аутентификация на основе паролей, методы подбора паролей, средства и методы повышения защищенности ОС от подбора паролей.
4. Аутентификация на основе внешних носителей ключа, биометрических характеристик пользователя.
5. Примеры реализации идентификации и аутентификации в современных ОС.
6. POSIX-совместимые операционные системы. Особенности архитектуры. История развития. Общая характеристика языка командного интерпретатора POSIX-совместимых ОС.
7. Переменные языка командного интерпретатора POSIX-совместимых ОС и их использование. Встроенные переменные

Контрольная работа №5

1. Управление порядком выполнения действий в языке командного интерпретатора POSIX-совместимых ОС. Команды для работы с файлами, каталогами, процессами, перенаправление ввода-вывода.
2. Отладка сценариев. Назначение и функции систем выполнения сценариев Windows. Объектные модели и языки систем выполнения сценариев ОС Windows.
3. Удаленное выполнение сценариев ОС Windows. Цифровая подпись сценариев в ОС Windows.
4. Классификация угроз безопасности ОС. Наиболее распространенные угрозы.
5. Понятие защищенной ОС.
6. Подходы к организации защиты. Этапы построения защиты. Административные меры защиты.
7. Стандарты безопасности ОС. Виртуальные машины. Изоляция процессов и пользователей.

Контрольная работа №6

1. Политики безопасности в ОС Windows
2. Субъекты, объекты, методы и права доступа. Привилегии субъектов доступа.
3. Избирательное и полномочное разграничение доступа, изолированная программная среда. Примеры реализации разграничения доступа в современных ОС.
4. Понятия идентификации, аутентификации и учета. Аутентификация на основе паролей, методы подбора паролей, средства и методы повышения защищенности ОС от подбора паролей
5. Аутентификация на основе внешних носителей ключа, биометрических характеристик пользователя. Примеры реализации идентификации, аутентификации и учета в современных ОС.
6. Необходимость аудита. Требования к подсистеме аудита.
7. Централизованный аудит. Штатный аудит в ОС Windows.
8. Реализации аудита в современных ОС.

Вопросы к экзамену по дисциплине «Безопасность операционных систем»

1. Основные понятия и положения защиты информации в информационно-вычислительных системах.
2. Предмет защиты информации.
3. Основные положения безопасности информационных систем.
4. Основные принципы обеспечения информационной безопасности в информационных системах
5. Угрозы безопасности информации в информационно-вычислительных системах

6. Анализ угроз информационной безопасности.
7. Методы обеспечения информационной безопасности.
8. Классификация злоумышленников
9. Основные направления и методы реализации угроз информационной безопасности.
10. Угрозы безопасности ОС.
11. 11 .Классификация угроз безопасности ОС. Наиболее распространенные угрозы
12. Программно-технический уровень информационной безопасности
13. Основные понятия программно-технического уровня информационной безопасности.
14. Требования к защите компьютерной информации. Классификация требований к системам защиты.
15. Формализованные требования к защите информации от НСД.
16. Общие подходы к построению систем защиты компьютерной
17. информации.
18. Различия требований и основополагающих механизмов защиты от НСД
19. Требования к защите ОС.
20. Понятие защищенной ОС.
21. Подходы к организации защиты ОС и их недостатки.
22. Этапы построения защиты. Административные меры защиты.
23. Стандарты безопасности ОС
24. Анализ выполнения современными ОС формализованных требований к защите информации от НСД.
25. Анализ существующей статистики угроз для современных универсальных ОС
26. Избирательное и полномочное разграничение доступа, изолированная программная среда. Примеры реализации разграничения доступа в современных ОС
27. Понятия идентификации и аутентификации пользователей.
28. Аутентификация на основе паролей, методы подбора паролей, средства и методы повышения защищенности ОС от подбора паролей.
29. Аутентификация на основе внешних носителей ключа, биометрических характеристик пользователя.
30. Примеры реализации идентификации и аутентификации в современных ОС.
31. P081X-совместимые операционные системы. Особенности архитектуры. История развития. Общая характеристика языка командного интерпретатора POSIX-совместимых ОС.
32. Переменные языка командного интерпретатора POSIX-совместимых ОС и их использование. Встроенные переменные
33. Управление порядком выполнения действий в языке командного интерпретатора POSIX-совместимых ОС. Команды для работы с файлами, каталогами, процессами, перенаправление ввода-вывода.
34. 34.Отладка сценариев. Назначение и функции систем выполнения сценариев Windows. Объектные модели и языки систем выполнения сценариев ОС Windows.
35. Удаленное выполнение сценариев ОС Windows. Цифровая подпись сценариев в ОС Windows.
36. Классификация угроз безопасности ОС. Наиболее распространенные угрозы.
37. Понятие защищенной ОС.
38. Подходы к организации защиты. Этапы построения защиты. Административные меры защиты.
39. Стандарты безопасности ОС. Виртуальные машины. Изоляция процессов и пользователей.
40. Политики безопасности в ОС Windows
41. Аутентификация на основе внешних носителей ключа, биометрических характеристик пользователя. Примеры реализации идентификации, аутентификации и учета в современных ОС.

42. Централизованный аудит. Штатный аудит в ОС Windows.
43. Реализации аудита в современных ОС.

Вопросы для контроля остаточных знаний по дисциплине «Безопасность операционных систем»

1. Основные понятия и положения защиты информации в информационно-вычислительных системах.
2. Основные положения безопасности информационных систем.
3. Основные принципы обеспечения информационной безопасности в информационных системах
4. Основные направления и методы реализации угроз информационной безопасности.
5. Основные понятия программно-технического уровня информационной безопасности.
6. Методы обеспечения информационной безопасности.
7. Субъекты, объекты, методы и права доступа. Привилегии субъектов доступа.
8. Понятие защищенной ОС.
9. Стандарты безопасности ОС.
10. Подходы к организации защиты ОС и их недостатки.
11. Общие подходы к построению систем защиты компьютерной информации.
12. Понятия идентификации и аутентификации пользователей.
13. Политики безопасности в ОС Windows
14. Реализации аудита в современных ОС

7. Учебно-методическое и информационное обеспечение дисциплины

Рекомендуемая литература и источники информации (основная и дополнительная) по дисциплине «Безопасность операционных систем»

№ п/п	Виды занятий	Комплект необходимой учебной литературы по дисциплине	Автор	Издат. и год изд.	Количество пособий, учебников и прочей литературы	
					В библ.	На каф.
Основная литература						
1.	ЛЗ, ЛБ, СРС	Метода и средства защиты информации в компьютерных системах: учебное пособие для студ. высш. учеб. заведений	Хорев П.Б.	М: Издательский центр «Академия», 2007. – 256с	50	1
2.	ЛЗ, ЛБ, СРС	Основы операционных систем [Электронный ресурс]	К. А. Коньков, В. Е. Карпов.	М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 346 с. — 2227-8397	http://www.iprbookshop.ru/73693.html	
3.	ЛЗ, ЛБ, СРС	Средства безопасности операционной системы Windows Server 2008 [Электронный ресурс]	Глотина, И. М.	Саратов: Вузовское образование, 2018. — 141 c. — 978-5-4487-0136-8.	http://www.iprbookshop.ru/72538.html	
4.	ЛЗ, ЛБ, СРС	Средства безопасности операционной системы Windows Server 2008 [Электронный ресурс]	Глотина, И. М.	Саратов : Вузовское образование, 2018. — 141 c. — 978-5-4487-0136-8.	http://www.iprbookshop.ru/72538.html	
5.	ЛЗ, ЛБ, СРС	Средства безопасности операционной системы ROSA Linux [Электронный ресурс]	Ложников, П. С.	Омск : Омский государственный технический университет, 2017. — 94 c. — 978-5-8149-2502-2	http://www.iprbookshop.ru/78474.html	
6.	ЛЗ, ЛБ, СРС	Сетевые операционные системы : учебник для вузов -	В.Г. Олифер, Н.А. Олифер.	СПб : Питер, 2005. - 544 с. : ил	10	1
7.	ЛЗ, ЛБ, СРС	Операционные системы: учеб.	Г.Х. Ирзаев	МО и Н РФ ГОУ ВПО "ДГТУ", Кафедра "ИСЭ". - Махачкала : Формат, 2011.	10	1
Дополнительная литература						
8.	ЛЗ, ЛБ, СРС	Операционная система Microsoft Windows XP. Русская версия [Электронный ресурс]	Ай Пи Эр Медиа.	М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2019. — 374 c. — 978-5-4486-0514-7.	http://www.iprbookshop.ru/79715.html	
9.	ЛЗ, ЛБ, СРС	Операционные системы. Часть 1 [Электронный ресурс] : учебное пособие	Грищенко, Ю. Б.	Томск: Томский государственный университет систем управления и радиоэлектроники, 2009. — 187 c. —	http://www.iprbookshop.ru/13952.html	

16

8.Материально-техническое обеспечение дисциплины

Для проведения лекционных занятий на факультете имеется комплект технических средств обучения в составе:

- интерактивная доска;

– переносной компьютер (в конфигурации не хуже: процессор IntelCore 2 Duo, 2 Гбайта ОЗУ, 500 Гбайт НЖМД);

– проектор (разрешение не менее 1280x1024);

Для проведения лабораторных занятий имеется компьютерный класс, оборудованный компьютерами с установленным программным обеспечением, предусмотренным программой дисциплины.

Программа составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем»

Рецензент от выпускающей кафедры (работодателя)
по специальности _____ подпись З.Р. Рагимбекова ФИО

Дополнения и изменения в рабочей программе
на 20__/___ учебный год

В рабочую программу вносятся следующие изменения

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Рабочая программа пересмотрена и одобрена на заседании кафедры _____20

Заведующий кафедрой _____

Внесенные изменения утверждаю
Проректор
по учебной работе _____

(декан) _____