МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Факультет информатики и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Безопасность операционных систем

Кафедра **Информатики и информационных технологий**
факультета **Информатики и информационных технологий**

Образовательная программа
10.03.01 Информационная безопасность

Профиль подготовки: Безопасность компьютерных систем

Уровень высшего образования: бакалавриат

Форма обучения
Очная

Статус дисциплины: вариативная

Махачкала, 2018

Рабочая программа дисциплины Безопасность операционных систем составлена в 2018 году в соответствии требованиями ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность (уровень бакалавриата) от « 01» декабря 2016 г. № 1515

Разработчик: каф. информатики и информационных технологий Гаджиев А.М., кандидат физ. – мат. наук, доцент.

Рабочая программа дисциплины одобрена:
на заседании информатики и информационных технологий

от « 02 » июля 2018г. протокол №12

Зав. кафедрой _____ Ахмедов С.А.
(подпись)

На заседании Методической комиссии Информатики и информационных технологий факультета от

« 03 » июля 2018г., протокол № 10

Председатель _____ Камилов К.Б.

(подпись)

Рабочая программа дисциплины согласована с учебно-методическим управлением

« 18 » 08 2018 г. _____

(подпись)

Аннотация рабочей программы дисциплины

Дисциплина Безопасность операционных систем входит в вариативную часть образовательной программы бакалавриата по направлению **10.03.01** Информационная безопасность

Дисциплина реализуется на факультете Информатики и информационных технологий кафедрой Информатики и информационных технологий.

Содержание дисциплины направлено теоретически и практически подготовить бакалавра к организации и проведению мероприятий по выявлению организации защиты основных используемых операционных систем и данных.

Служит, прежде всего, для формирования определенного мировоззрения в информационной сфере безопасности и освоения информационной культуры, т.е. умения целенаправленно работать с информацией, применять всевозможные информационные технологии, используя их для решения профессиональных вопросов.

Дисциплина нацелена на формирование следующих компетенций выпускника: профессиональных –ПК-1, ПК-2, ПК-3, ПК-4, ПК-6, ПК-13, ПК-14, ПК-15.

Преподавание дисциплины предусматривает проведение следующих видов учебных занятий в 7 семестре:

лекции, практические занятия, лабораторные занятия, самостоятельная работа.

Рабочая программа дисциплины предусматривает проведение следующих видов контроля успеваемости в форме модульных контрольных работ и промежуточный контроль в форме зачета

Объем дисциплины 6 зачетных единиц, в том числе в академических часах по видам учебных занятий

Семестр	Учебные занятия								Форма промежуточной аттестации (зачет, дифференцированный зачет, экзамен
	в том числе:								
	всего	Контактная работа обучающихся с преподавателем						СРС, в том числе экзамен	
		всего	из них						
			Лекции	Лабораторные занятия	Практические занятия	КСР	контроль		
7	108	56	20	18	18			52	зачет

1. Цели освоения дисциплины

Целью дисциплины «Безопасность операционных систем» является формирование у студентов знаний по основам безопасности операционных систем и их компонентов.

Кроме того, целью дисциплины является развитие в процессе обучения системного мышления, необходимого для решения задач программной защиты информации с учетом требований системного подхода.

Дисциплина «Безопасность операционных систем» имеет целью обучить студентов принципам построения защиты информации в ОС и анализа надежности защиты ОС.

2.Место дисциплины в структуре ОПОП бакалавриата

Дисциплина «Безопасность операционных систем» входит в вариативную часть образовательной программы бакалавриата по направлению (специальности) **10.03.01** «Информационная безопасность».

Курс «Безопасность операционных систем» предусмотрен Федеральным государственным общеобразовательным стандартом высшего образования РФ и предназначен для бакалавров, обучающихся по направлению **10.03.01**«Информационная безопасность». Дисциплина «Информационные технологии» относится к блоку Математических и естественнонаучных дисциплин, вариативной части. Общая трудоемкость курса 108часов, в том числе аудиторных занятий – 56 часов. Аудиторные занятия включают в себя лекции, лабораторные и практические занятия. Самостоятельная работа (52 часа) студентов состоит в самостоятельном изучении отдельных тем по учебной программе. Лабораторные, практические занятия, а также самостоятельная работа оцениваются и комментируются по мере выполнения.

Дисциплина «Безопасность операционных систем» относится к базовой части профессионального цикла. Её изучение базируется на следующих дисциплинах:

«Операционные системы».

В результате изучения дисциплины студенты должны иметь представление:

Знать:

- требования к защищенным ОС;
- критерии оценки эффективности и надежности средств защиты ОС;
- принципы организации и структуру подсистем защиты ОС семейств Unix и Windows;
-критерии и методы оценивания механизмов защиты.

Уметь:

оценивать эффективность и надежность защиты ОС;

выявлять слабости защиты ОС и использовать их для вскрытия защиты;

планировать политику безопасности ОС;

пользоваться средствами защиты, предоставляемыми ОС;

проводить анализ и оценивание механизмов защиты.

***Владеть**:*

навыками построения защиты ОС Windows, Unix.

1. Компетенции обучающегося, формируемые в результате освоения дисциплины (перечень планируемых результатов обучения).

Код компетенции из ФГОС ВО	Наименование компетенции из ФГОС ВО	Планируемые результаты обучения
ПК-1	способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	*Знает:* положения политики безопасности операционных систем *Умеет:* настраивать основные компоненты политики безопасности операционных систем *Владеет:* методами и регламентом компонентов политики безопасности операционных систем
ПК-2	способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	*Знает:* программные средства и приложения используемые для защиты основных компонентов операционных систем *Умеет:* применять на практике методы и компоненты защиты операционных систем *Владеет:* способами защиты операционных систем во внештатных ситуациях
ПК-3	способностью администрировать подсистемы информационной безопасности объекта защиты	*Знает:* основные положения сбора информации и проведения анализа при организации защиты операционных систем *Умеет:* анализировать сложившуюся ситуацию при организации защиты операционных систем *Владеет:* способами и методами анализа защищенности операционных систем
ПК-4	способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению	*Знает:* методы и основные пункты политики безопасности операционных систем *Умеет:* применять методы комплексного подхода политики безопасности операционных систем

	информационной безопасности объекта защиты	*Владеет:* способами комплексного подхода при обеспечении политики безопасности в различных сферах
ПК-6	способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	*Знает:* основные способы и методы проведении контрольных проверок работоспособности и эффективности программных, программно-аппаратных и технических средств защиты информации *Умеет:* проводить контрольные проверки работоспособности оборудования *Владеет:* навыками позволяющие быстро и эффективно проводить контрольные проверки
ПК-13	способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	*Знает:* необходимый перечень мер по обеспечению информационной безопасности *Умеет:* организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности *Владеет:* управлением процесса реализации по обеспечению информационной безопасности
ПК-14	способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности	*Знает:* основные методы организации работы малого коллектива исполнителей в профессиональной деятельности *Умеет:* организовывать работу малого коллектива исполнителей *Владеет:* техникой, корректностью и тактом в общении с подчиненными
ПК-15	способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	*Знает:* нормативные правовые акты и нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю *Умеет:* организовывать технологический процесс защиты информации ограниченного доступа *Владеет:* организаторскими навыками организации технологического процесса защиты информации ограниченного доступа

4. Объем, структура и содержание дисциплины.

4.1. Объем дисциплины составляет 3 зачетные единицы, 56 академических часа.

4.2. Структура дисциплины.

№ п/п	Разделы и темы дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Самостоятельная работа	Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные занятия	Контроль самост. раб.		
	Модуль 1. ***Концепции защиты операционных систем***								
1	Основные понятия и положения защиты информации в информационно-вычислительных системах	7	1	4	2	2		4	
2	Угрозы безопасности информации в информационно-вычислительных системах	7	2	2	2	2		6	
3	Угрозы безопасности ОС	7	5	2	2	2		6	
	Итого по модулю 1:			8	6	6		16	36
	Модуль 2. ***Теоретические основы защиты операционных систем***								
1	Программно-технический уровень информационной безопасности	7	7	2	2	2		6	
2	Анализ защищенности современных операционных систем.	7	9	2	2	2		6	
3	Встроенные средства защиты Windows, Unix	7	11	2	2	2		6	
	Итого по модулю 2:			6	6	6		18	36
	Модуль 3. ***Реализация защиты операционных систем***								
1	Обзор и статистика методов, лежащих в основе атак на современные ОС.	7	13	2	2	2		6	
2	Разграничение доступа в ОС	7	15	2	2	2		6	
3	Защита сетевого взаимодействия	7	17	2	2	2		6	

	Windows, Unix								
	Итого по модулю 3:			6	6	6		18	36
	ИТОГО:			20	18	18		52	108

4.3. Содержание дисциплины, структурированное по темам (разделам).

4.3.1. Содержание лекционных занятий по дисциплине

Модуль 1. ***Концепции защиты операционных систем***

Тема 1.1. 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.

Тема 1.2. Угрозы безопасности информации в информационно-вычислительных системах

Анализ угроз информационной безопасности. Методы обеспечения информационной безопасности. Классификация злоумышленников. Основные направления и методы реализации угроз информационной безопасности.

Тема 1.3. Угрозы безопасности ОС.

Классификация угроз безопасности ОС. Наиболее распространенные угрозы.

Тема 1.4. Программно-технический уровень информационной безопасности

Основные понятия программно-технического уровня информационной безопасности. Требования к защите компьютерной информации. Классификация требований к системам защиты. Формализованные требования к защите информации от НСД. Общие подходы к построению систем защиты компьютерной информации. Различия требований и основополагающих механизмов защиты от НСД.

Модуль 2. ***Теоретические основы защиты операционных систем***

Тема 2.1. Требования к защите ОС.

Понятие защищенной ОС. Подходы к организации защиты ОС и их недостатки. Этапы построения защиты. Административные меры защиты. Стандарты безопасности ОС.

Тема 2.2. Анализ защищенности современных операционных систем.

Анализ выполнения современными ОС формализованных требований к защите информации от НСД. Анализ существующей статистики угроз для современных универсальных ОС.

Тема 2.3. Обзор и статистика методов, лежащих в основе атак на современные ОС.

Классификация методов и их сравнительная статистика.

Модуль 3. ***Реализация защиты операционных систем***

Тема 3.1. Разграничение доступа в ОС.

Субъекты, объекты, методы и права доступа. Привилегии субъектов доступа. Избирательное и полномочное разграничение доступа, изолированная программная среда. Примеры реализации разграничения доступа в современных ОС.

Тема 3.2. Идентификация и аутентификация пользователей ОС.

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.

4.3.2. ***Содержание лабораторно-практических занятий по дисциплине.***

Модуль 1. ***Концепции защиты операционных систем***

Тема 1.1. Разграничение доступа к ресурсам в ОС Windws, Unix.

Организация разграничения доступа к объектам в Windows XP и Windows 2003. Разделяемые сетевые ресурсы, NTFS и права доступа. Распределенная файловая система (DFS) и права доступа. Назначение прав доступа к объектам: файлам и папкам NTFS, сетевым ресурсам, объектам Active Directory.

Тема 1.2. Аудит в ОС.

Необходимость аудита. Требования к подсистеме аудита. Примеры реализации аудита в современных ОС.

Тема 1.3. Защита сетевого взаимодействия Windows, Unix.

Методика проникновения. Сбор информации о системе. Защита каналов средствами Windows XP/2003/Vista, Windows Firewall. Виртуальные частные сети, протоколы L2TP и PPTP. Обзор защиты беспроводных сетей (Wi-Fi) в Windows XP/Vista.

Темы лабораторных работ

1. Анализ защищенности операционных систем семейства Windows.
2. Анализ защищенности операционных систем семейства Unix.
3. Изучение защитных механизмов, реализованных в Windows XP/2003/Vista.

Модуль 2. ***Теоретические основы защиты операционных систем***

Тема 2.1. Повышение уровня защищенности рабочей среды пользователей на базе Windows.

Безопасность рабочей среды и приложений пользователя. Настройки зон безопасности. Безопасность приложений с поддержкой сценариев. Централизованная настройка приложений через групповые политики. Защита от неправомерных изменений конфигурации рабочих станций и серверов, от использования неучтенных программ (замкнутая программная среда).

Тема 2.2. Повышение уровня защищенности рабочей среды пользователей на базе Unix.

Тема 2.3. Анализ параметров безопасности и конфигурирование безопасности систем под управлением Windows, Unix.

Темы лабораторных работ

1. Применение шаблонов безопасности для защиты рабочих станций пользователей под управлением Windows XP/Vista.
2. Защита серверов под управлением Windows 2003 с использованием Security configuration wizard.
3. Анализ параметров безопасности с использованием Security Configuration and Analysis.

Модуль 3. ***Реализация защиты операционных систем***

Тема 3.1. Повышение защищенности служб на базе Windows, Unix

Тема 3.2. Защита Active Directory. Защита DNS, FTP, DHCP. Защита терминального сервера с использованием RDP.

Тема 3.3. Изучение средств защиты сетевого взаимодействия Windows. Конфигурирование средств защиты каналов средствами Windows XP/2003/Vista, Windows Firewall. Виртуальные частные сети, протоколы L2TP и PPTP.

Темы лабораторных работ

1. Исследование методов идентификации и аутентификации в ОС Windows. Исследование методов разграничение доступа к ресурсам в ОС Windws, Unix
2. Изучение средств защиты сетевого взаимодействия Windows. Конфигурирование средств защиты каналов средствами Windows XP/2003/Vista, Windows Firewall. Виртуальные частные сети, протоколы L2TP и PPTP.
3. Применение карантина для обеспечения безопасности мобильных пользователей на Windows XP/Vista.

5. Образовательные технологии

Рекомендуемые образовательные технологии: лекции, практические лабораторные занятия, самостоятельная работа студентов.

- В соответствии с требованиями ФГОС ВПО по направлению подготовки реализация компетентностного подхода предусматривает широкое использование в учебном процессе активных и интерактивных форм проведения занятий (компьютерных симуляций, разбор конкретных ситуаций) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.
- Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью (миссией) программы, особенностью контингента обучающихся и содержанием конкретных дисциплин, и в целом в учебном процессе они должны составлять не менее 30% аудиторных занятий (определяется требованиями ФГОС с учетом специфики ООП). Занятия лекционного типа для соответствующих групп студентов не могут составлять более 60% аудиторных занятий (определяется соответствующим

ФГОС)).

Вид Технология занятия		Цель	Формы и методы обучения
1	2	3	4
Лекции	Технология проблемного обучения	Усвоение теоретических знаний, развитие мышления, формирование профессионального интереса к будущей деятельности	Мультимедийные лекция-объяснение, лекция-визуализация, с привлечением формы тематической дискуссии, беседы, анализа конкретных ситуаций
Лабораторные работы (компьютерный практикум)	Технология проблемного, модульного, дифференцированного и активного обучения, деловой игры	Развитие творческой и познавательной самостоятельности, обеспечение индивидуального подхода с учетом базовой подготовки. Организация активности студентов, обеспечение личностно деятельного характера усвоения знаний, приобретения навыков, умений.	Индивидуальный темп обучения. Постановка проблемных познавательных задач. Методы активного обучения: «круглый стол», игровое производственное проектирование, анализ конкретных ситуаций.
Самостоятельная работа	Технологии концентрированного, модульного, дифференцированного обучения	Развитие познавательной самостоятельности, обеспечение гибкости обучения, развитие навыков работы с различными источниками информации, развитие умений, творческих	Индивидуальные, групповые, интерактивные (в режимах on-line и off-line).

6.Учебно-методическое обеспечение самостоятельной работы студентов.

Методические рекомендации студентам по организации самостоятельной работы при изучении дисциплины «Информационные технологии»

При подготовке к коллоквиуму, зачету каждый студент должен индивидуально готовиться по темам дисциплины, читая конспекты лекций и рекомендуемую учебную и справочную литературу, усваивая определения, схемы и принципы соответствующих расчетов. Самостоятельная работа позволяет студенту в спокойной обстановке подумать и разобраться с информацией по теме, структурировать знания. Чтобы содержательная информация по дисциплине запоминалась надолго, целесообразно изучать ее поэтапно, в предлагаемой последовательности, поскольку последующий материал связан с предыдущим. По каждой из тем для самостоятельного изучения, приведенных в рабочей программе дисциплины следует сначала прочитать рекомендованную литературу и при необходимости составить краткий конспект основных положений, терминов, сведений, требующих запоминания и являющихся основополагающими в этой теме и для освоения последующих разделов курса.

При выполнении индивидуальных заданий студент использует приобретенные на практических занятиях навыки расчетов, самостоятельно изучает примеры из лекций. Самостоятельная работа при выполнении индивидуальных заданий требует изучения и использования справочных материалов. Залогом успеха в приобретении знаний и навыков по дисциплине является синхронизация выполняемых индивидуальных заданий по срокам с лекционным материалом и разбираемым на практических занятиях.

1. Основные понятия и положения защиты информации в информационно-вычислительных системах
2. Угрозы безопасности информации в информационно-вычислительных системах
3. Угрозы безопасности ОС
4. Программно-технический уровень информационной безопасности
5. Требования к защите ОС
6. Анализ защищенности современных операционных систем. Встроенные средства защиты Windows, Unix
7. Обзор и статистика методов, лежащих в основе атак на современные ОС.
8. Разграничение доступа в ОС
9. Идентификация и аутентификация пользователей ОС
10. Разграничение доступа к ресурсам в ОС Windws, Unix
11. Аудит в ОС
12. Защита сетевого взаимодействия Windows, Unix
13. Повышение уровня защищенности рабочей среды пользователей на базе Windows
14. Повышение уровня защищенности рабочей среды пользователей на

базе Unix

15.Анализ параметров безопасности и конфигурирование безопасности систем под управлением Windows, Unix

16.Повышение защищенности служб на базе Windows, Unix

17.Системы защиты программного обеспечения

Методические рекомендации по самостоятельной подготовке к лабораторным, практическим занятиям

1. Предмет защиты информации. Основные положения безопасности информационных систем. Основные принципы обеспечения информационной безопасности в информационных системах.
2. Угрозы безопасности ОС. Классификация угроз безопасности ОС. Наиболее распространенные угрозы.
3. Требования к защите ОС. Понятие защищенной ОС. Подходы к организации защиты. Этапы построения защиты. Административные меры защиты. Стандарты безопасности ОС.
4. Основные понятия программно-технического уровня информационной безопасности.
5. Требования к защите компьютерной информации. Классификация требований к системам защиты. Формализованные требования к защите информации от НСД.
6. Общие подходы к построению систем защиты компьютерной информации. Различия требований и основополагающих механизмов защиты от НСД.
7. Требования к защите ОС. Понятие защищенной ОС. Подходы к организации защиты ОС и их недостатки. Этапы построения защиты. Административные меры защиты. Стандарты безопасности ОС.
8. Разграничение доступа в ОС. Субъекты, объекты, методы и права доступа. Привилегии субъектов доступа. Избирательное и полномочное разграничение доступа, изолированная программная среда. Примеры реализации разграничения доступа в современных ОС.
9. Идентификация и аутентификация пользователей ОС. 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.
10. Аудит в ОС. Необходимость аудита. Требования к подсистеме аудита. Примеры реализации аудита в современных ОС.
11. Системы защиты программного обеспечения.

Вопросы для самоконтроля

7. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.
Перечень компетенций с указанием этапов их формирования приведен в описании образовательной программы.

Код компетенции из ФГОС ВО	**Наименование компетенции из ФГОС ВО**	**Планируемые результаты обучения**	**Процедура освоения**
ПК-1	способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	*Знает:* положения политики безопасности операционных систем *Умеет:* настраивать основные компоненты политики безопасности операционных систем *Владеет:* методами и регламентом компонентов политики безопасности операционных систем	Устный опрос, сдача лабораторных работ, контрольная работа
ПК-2	способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	*Знает:* программные средства и приложения используемые для защиты основных компонентов операционных систем *Умеет:* применять на практике методы и компоненты защиты операционных систем *Владеет:* способами защиты операционных систем во внештатных ситуациях	Устный опрос, сдача лабораторных работ, контрольная работа
ПК-3	способностью администрировать подсистемы информационной безопасности объекта защиты	*Знает:* основные положения сбора информации и проведения анализа при организации защиты операционных систем *Умеет:* анализировать сложившуюся ситуацию при организации защиты операционных систем *Владеет:* способами и методами анализа защищенности операционных систем	Устный опрос, сдача лабораторных работ, контрольная работа
ПК-4	способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной	*Знает:* методы и основные пункты политики безопасности операционных систем *Умеет:* применять методы комплексного подхода политики безопасности операционных систем *Владеет:* способами комплексного	Сдача лабораторных работ, контрольная работа

	безопасности объекта защиты	подхода при обеспечении политики безопасности в различных сферах	
ПК-6	способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	*Знает:* основные способы и методы проведении контрольных проверок работоспособности и эффективности программных, программно-аппаратных и технических средств защиты информации *Умеет:* проводить контрольные проверки работоспособности оборудования *Владеет:* навыками позволяющие быстро и эффективно проводить контрольные проверки	Сдача лабораторных работ, контрольная работа
ПК-13	способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	*Знает:* необходимый перечень мер по обеспечению информационной безопасности *Умеет:* организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности *Владеет:* управлением процесса реализации по обеспечению информационной безопасности	Устный опрос, сдача лабораторных работ, контрольная работа
ПК-14	способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности	*Знает:* основные методы организации работы малого коллектива исполнителей в профессиональной деятельности *Умеет:* организовывать работу малого коллектива исполнителей *Владеет:* техникой, корректностью и тактом в общении с подчиненными	Сдача лабораторных работ
ПК-15	способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	*Знает:* нормативные правовые акты и нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю *Умеет:* организовывать технологический процесс защиты информации ограниченного доступа *Владеет:* организаторскими навыками организации технологического процесса защиты информации ограниченного доступа	Устный опрос, сдача лабораторных работ, контрольная работа

7.2. Типовые контрольные тесы

Вопросы промежуточной (модульной) аттестации

Модуль 1. ***Концепции защиты операционных систем***

1. Предмет защиты информации.
2. Основные положения безопасности информационных систем.
3. Основные принципы обеспечения информационной безопасности в информационных системах.
4. Анализ угроз информационной безопасности.
5. Методы обеспечения информационной безопасности.
6. Классификация злоумышленников.
7. Основные направления и методы реализации угроз информационной безопасности.
8. Основные понятия программно-технического уровня информационной безопасности.
9. Требования к защите компьютерной информации.
10. Классификация требований к системам защиты.
11. Формализованные требования к защите информации от НСД.
12. Общие подходы к построению систем защиты компьютерной информации.
13. Различия требований и основополагающих механизмов защиты от НСД.

Модуль 2. ***Теоретические основы защиты операционных систем***

1. Понятие защищенной ОС.
2. Подходы к организации защиты ОС и их недостатки.
3. Этапы построения защиты.
4. Административные меры защиты.
5. Стандарты безопасности ОС.
6. Анализ выполнения современными ОС формализованных требований к защите информации от НСД.
7. Анализ существующей статистики угроз для современных универсальных ОС.
8. Классификация методов и их сравнительная статистика.

Модуль 3. ***Реализация защиты операционных систем***

1. Субъекты, объекты, методы и права доступа.
2. Привилегии субъектов доступа.
3. Избирательное и полномочное разграничение доступа, изолированная программная среда.
4. Примеры реализации разграничения доступа в современных ОС.
5. Понятия идентификации и аутентификации пользователей.
6. Аутентификация на основе паролей, методы подбора паролей, средства и методы повышения защищенности ОС от подбора паролей.

7. Аутентификация на основе внешних носителей ключа, биометрических характеристик пользователя.
8. Примеры реализации идентификации и аутентификации в современных ОС.

Типовые тестовые вопросы:

1. Угрозы безопасности ОС
2. Программно-технический уровень информационной безопасности
3. Требования к защите ОС
4. Анализ защищенности современных операционных систем. Встроенные средства защиты Windows, Unix
5. Обзор и статистика методов, лежащих в основе атак на современные ОС.
6. Идентификация и аутентификация пользователей ОС
7. Разграничение доступа к ресурсам в ОС Windws, Unix
8. Аудит в ОС
9. Защита сетевого взаимодействия Windows, Unix
10. Повышение уровня защищенности рабочей среды пользователей на базе Windows
11. Повышение уровня защищенности рабочей среды пользователей на базе Unix
12. Анализ параметров безопасности и конфигурирование безопасности систем под управлением Windows, Unix
13. Повышение защищенности служб на базе Windows, Unix
14. Системы защиты программного обеспечения
15. Предмет защиты информации.
16. Основные положения безопасности информационных систем.
17. Основные принципы обеспечения информационной безопасности в информационных системах.
18. Угрозы безопасности ОС.
19. Классификация угроз безопасности ОС.
20. Наиболее распространенные угрозы.
21. Требования к защите ОС.
22. Понятие защищенной ОС.
23. Подходы к организации защиты.
24. Этапы построения защиты.
25. Административные меры защиты.
26. Стандарты безопасности ОС.
27. Основные понятия программно-технического уровня информационной безопасности.
28. Требования к защите компьютерной информации.
29. Классификация требований к системам защиты.
30. Формализованные требования к защите информации от НСД.

31. Общие подходы к построению систем защиты компьютерной информации.
32. Различия требований и основополагающих механизмов защиты от НСД.
33. Требования к защите ОС.
34. Понятие защищенной ОС.
35. Подходы к организации защиты ОС и их недостатки.
36. Этапы построения защиты.
37. Административные меры защиты.
38. Стандарты безопасности ОС.
39. Разграничение доступа в ОС.
40. Субъекты, объекты, методы и права доступа.
41. Привилегии субъектов доступа.
42. Избирательное и полномочное разграничение доступа, изолированная программная среда.
43. Примеры реализации разграничения доступа в современных ОС.
44. Идентификация и аутентификация пользователей ОС.
45. Понятия идентификации и аутентификации пользователей.
46. Аутентификация на основе паролей,
47. Методы подбора паролей,
48. Средства и методы повышения защищенности ОС от подбора паролей.
49. Аутентификация на основе внешних носителей ключа, биометрических характеристик пользователя.
50. Примеры реализации идентификации и аутентификации в современных ОС.
51. Аудит в ОС.
52. Необходимость аудита.
53. Требования к подсистеме аудита.
54. Примеры реализации аудита в современных ОС.
55. Системы защиты программного обеспечения.

7.3. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Программой дисциплины в целях проверки прочности усвоения материала предусматривается проведение различных форм контроля:

1. «Входной» контроль определяет степень сформированности знаний, умений и навыков обучающегося, необходимым для освоения дисциплины и приобретенным в результате освоения предшествующих дисциплин.

2. Тематический контроль определяет степень усвоения обучающимися каждого раздела (темы в целом), их способности связать учебный материал с уже усвоенными знаниями, проследить развитие, усложнение явлений, понятий, основных идей.

3. Межсессионная аттестация– рейтинговый контроль знаний студентов, проводимый в середине семестра.

4. Рубежной формой контроля является зачет. Изучение дисциплины завершается зачетом, проводимым в виде письменного опроса с учетом текущего рейтинга.

Рейтинговая оценка знаний студентов проводится по следующим критериям:

Вид оцениваемой учебной работы студента	Баллы за единицу работы	Максимальное значение
Посещение всех лекции	макс. 5 баллов	5
Присутствие на всех практических занятиях	макс. 5 баллов	5
Оценивание работы на семинарских, практических, лабораторных занятиях	макс. 10 баллов	10
Самостоятельная работа	макс. 40 баллов	40
Итого		60

Неявка студента на промежуточный контроль в установленный срок без уважительной причины оценивается нулевым баллом. Повторная сдача в течение семестра не разрешается.

Дополнительные дни отчетности для студентов, пропустивших контрольную работу по уважительной причине, подтвержденной документально, устанавливаются преподавателем дополнительно.

Лабораторные работы, пропущенные без уважительной причины, должны быть отработаны до следующей контрольной точки, если сдаются позже, то оцениваются в 1 балл.

Студенты, набравшие от 51 до 100 баллов, получают зачет по дисциплине без проведения дополнительных испытаний, если сумма набранных баллов меньше 50, то студент пишет итоговый тест по дисциплине в последнюю учебную неделю семестра.

Итоговой формой контроля знаний, умений и навыков по дисциплине является **(зачет)**.

Зачет проводится по тестам или в устной форме, которые включают 2 (два) вопроса теоретический, практический.

При соответствии ответа учащегося на зачете более чем 50 % критериев из этого списка выставляется оценка «зачет», в случае несоответствия – «незачет».

Вторым вариантом проведения зачета является проверка знаний учащихся с помощью с помощью электронных тестов, в этом случае оценка «зачет» ставится при правильном ответе как минимум на 60 % предложенных вопросов.

1. **Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.**

Основная литература

1. Ложников П.С. Обеспечение безопасности сетевой инфраструктуры на основеоперационных систем Microsoft [Электронный ресурс]: практикум/ Ложников П.С., Михайлов Е.М.— Электрон. текстовые данные.— Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017.— 264 c.— Режим доступа: http://www.iprbookshop.ru/67389.html.
2. Проскурин, Вадим Геннадьевич и др.
   Защита в операционных системах : Програм.-аппарат. средства обеспечения информ. безопасности: Учеб. пособие для вузов / Проскурин, Вадим Геннадьевич и др. ; С.В.Крутов, И.В.Мацкевич. - М. : Радио и связь, 2000. - 164,[2] с. : ил. - ISBN 5-256-01414-5 : 30-00.
   Местонахождение: Научная библиотека ДГУ URL
3. Гриценко Ю.Б. Операционные системы. Часть 2 [Электронный ресурс]: учебное пособие/ Гриценко Ю.Б.— Электрон. текстовые данные.— Томск: Томский государственный университет систем управления и радиоэлектроники, 2009.— 230 c.— Режим доступа: http://www.iprbookshop.ru/13953.html.

Дополнительная литература:

1. Нестеров С.А. Анализ и управление рисками в информационных системах на базе операционных систем Microsoft [Электронный ресурс] / С.А. Нестеров. — Электрон. текстовые данные. — М. : ИнтернетУниверситет Информационных Технологий (ИНТУИТ), 2016. — 250 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/52141.html
2. Мезенцева Е.М. Операционные системы [Электронный ресурс] : лабораторный практикум / Е.М. Мезенцева, О.С. Коняева, С.В. Малахов. — Электрон. текстовые данные. — Самара: Поволжский государственный университет телекоммуникаций и информатики, 2017. — 214 c. — 2227- 8397. — Режим доступа: http://www.iprbookshop.ru/75395.html
3. Смышляев А.Г. Информационная безопасность. Лабораторный практикум [Электронный ресурс] : учебное пособие / А.Г. Смышляев. — Электрон. текстовые данные. — Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, ЭБС АСВ, 2015. — 102 c. — 2227-8397. — Режим доступа:

http://www.iprbookshop.ru/66655.html

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.

news://comp.os.linux.misc/

www .kiev .epos.us

http://www.isu.kasib.ru

http://www.apcmedia.com/pdf_downloads/litpdfs/996-1751F.pdf

http://www.apcmedia.com/salestools/TDOY-5UQVCZ_R2_EN.pdf

http://sturgeon.apcc.com/techref.nsf/partnum/990-3029/$FILE/990-3029-EN.pdf

10. Методические указания для обучающихся по освоению дисциплины.

Студенты очной формы обучения нормативного срока обучения изучают дисциплину " Безопасность операционных систем" в течение 7 семестра. Виды и объем учебных занятий, формы контроля знаний приведены в табл. 1. Темы и разделы рабочей программы, количество лекционных часов и количество часов самостоятельной работы студентов на каждую из тем приведены в табл. 2. В первой колонке этой таблицы указаны номера тем согласно разделу 4. Организация лабораторного практикума, порядок подготовки к лабораторным занятиям и методические указания к самостоятельной работе студентов, а также порядок допуска к лабораторным занятиям и отчетности по проделанным работам определены в методических указаниях по выполнению лабораторных работ.

Самостоятельная работа студентов в ходе изучения лекционного материала заключается в проработке каждой темы в соответствии с методическими указаниями, а также в подготовке выполнения лабораторных работ, которые выдаются преподавателем на лекционных занятиях.

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем.

Программные продукты

- Операционная система: Операционные системы семействаWindows
- Microsoft Office.

Лабораторные занятие проводятся в классах персональных ЭВМ;

Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для организации образовательного процесса по дисциплине необходим компьютерный класс с локальной сетью и программы для виртуализации систем: VM Ware Workstation, Virtual PC, с возможность запуска образов виртуальных машин под управлением ОС Windows NT, FreeBSD и т.д.