Аннотация к рабочей программе дисциплины «Безопасность операционных систем»

Цель преподавания дисциплины

Целью преподавания дисциплины «Безопасность операционных систем» является получение студентами знаний о принципах построения, идеологии и архитектуре современных операционных систем, реализуемых в них механизмах защиты.

Задачи изучения дисциплины

Основными задачами изучения дисциплины является: получить знания о назначении, принципах функционирования и структуре операционных систем; получить знания о функционировании подсистемы управления процессами; получить знания о функционировании подсистем управления распределением ресурсов получить знания о функционировании подсистем управления памятью в различных операционных системах; получить знания о назначении, организации и функционировании файловых систем.

Знания и умения, которыми должен обладать студент, успешно освоивший данную дисциплину: знания о функционировании подсистемы устройствами ввода – вывода; знания о принципах организации операционных систем семейств Windows и UNIX получить знания о методах и средствах оценки производительности операционных систем, загруженности системных ресурсов; знания о механизмах защиты объектов, реализованных средствами операционной системы Windows.

Компетенции, формируемые в результате освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на

основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК–7)

− способность администрировать подсистемы информационной безопасности объекта защиты (ПК-3);

− способность учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации (ПСК-4.1);

− способность выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей (ПСК-4.2).

Разделы дисциплины

Понятие ОС, история, классификация, основные функции. Процессы, модель, состояния. Нити. Диспетчеризация и синхронизация процессов. Проблемы межпроцессного взаимодействия. Взаимоблокировки процессов. Управление памятью в ОС. Файловые системы. Механизмы защиты Управление вводом – выводом в ОС. Механизмы разграничения доступа в ОС. Механизмы безопасной работы в ОС. Администрирование ОС

МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
Декан факультета
фундаментальной и прикладной
(наименование ф-та полностью)
информатики

Т.А. Ширабакина
(подпись, инициалы, фамилия)
«1» февраля 2017 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Безопасность операционных систем

направление подготовки (специальность) *10.03.01*
(шифр согласно ФГОС
Информационная безопасность
и наименование направление подготовки (специальности)

Безопасность автоматизированных систем
наименование профиля, специализации или магистерской программы

форма обучения *очная*
очная, очно-заочная, заочная

Курск – 2017

Рабочая программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего профессионального образования по специальности *10.05.02 – «Информационная безопасность телекоммуникационных систем»* и на основании учебного плана по специальности *10.05.02 – «Информационная безопасность телекоммуникационных систем»* (профиль *«Защита информации в системах связи управления»*), одобренного Учёным советом университета, протокол №_5_ «30» 01 2017г.

Рабочая программа обсуждена и рекомендована к применению в учебном процессе для обучения студентов по специальности *10.05.02 – «Информационная безопасность телекоммуникационных систем»* на заседании кафедры информационной безопасности. Протокол №_9_ «_1_» 02 2017г.

И.о. зав. кафедрой ИБ Таныгин М.О.

Разработчик программы
доцент кафедры ИБ Таныгин М.О.

Согласовано:
Директор научной библиотеки Макаровская В.Г.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана по специальности *10.05.02 – «Информационная безопасность телекоммуникационных систем»*, одобренного Ученым советом университета протокол №_5_ «30» 01 2017г. на заседании кафедры информационной безопасности. Протокол №_1_ «_1_» 02 2018г.

Зав. кафедрой_____

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана по специальности *10.05.02 – «Информационная безопасность телекоммуникационных систем»*, одобренного Ученым советом университета протокол №_5_ «30» 01 2017г. на заседании кафедры информационной безопасности. Протокол №_12_ «_28_» 06 2018г.

Зав. Кафедрой_____ Таныгин М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана по специальности *10.05.02 – «Информационная безопасность телекоммуникационных систем»*, одобренного Ученым советом университета протокол №___ «___» _____20_ г. на заседании кафедры информационной безопасности. Протокол №_11_ «_25_» 06 20_1_г.

Зав. кафедрой_____ КТН доцент Таныгин М.О

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №7 «25» 02 2020 г. на заседании кафедры информационной безопасности. Протокол №1 от «31» 08 2020г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №7 «25» 02 2020 г. на заседании кафедры информационной безопасности. Протокол №11 от «28» 06 2021 г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №7 «25» 02 2020 г. на заседании кафедры информационной безопасности. Протокол №11 от «30» 06 2022 г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №__ «___» _____ 20__ г. на заседании кафедры информационной безопасности. Протокол №__ от «__»_____20__г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №__ «___» _____ 20__ г. на заседании кафедры информационной безопасности. Протокол №__ от «__»_____20__г.

Зав. кафедрой _____

1. Цель и задачи дисциплины. Перечень планируемых результатов обучения, соотнесённых с планируемыми результатами освоения образовательной программы

1.1. Цель преподавания дисциплины

Дисциплина «Безопасность операционных систем» является получение студентами знаний о принципах построения, идеологии и архитектуре современных операционных систем, реализуемых в них механизмах защиты.

1.2. Задачи изучения дисциплины

В результате изучения дисциплины студенты должны:

- получить знания о назначении, принципах функционирования и структуре операционных систем;
- получить знания о функционировании подсистемы управления процессами;
- получить знания о функционировании подсистем управления распределением ресурсов
- получить знания о функционировании подсистем управления памятью в различных операционных системах;
- получить знания о назначении, организации и функционировании файловых систем;
- получить знания о функционировании подсистемы устройствами ввода – вывода;
- получить знания о принципах организации операционных систем семейств Windows и UNIX
- получить знания о методах и средствах оценки производительности операционных систем, загруженности системных ресурсов.
- получить знания о механизмах защиты объектов, реализованных средствами операционной системы Windows.

1.3. Перечень планируемых результатов обучения, соотнесённых с планируемыми результатами освоения образовательной программы

Обучающиеся должны **знать:**

- принципы построения современных операционных систем;
- назначение, организацию и принципы функционировании файловых систем
- механизмы защиты объектов, реализованных средствами операционных систем

уметь:

- администрировать подсистемы управления доступа современных операционных систем

− устанавливать и настраивать операционные системы и их посистемы обеспечения информационной безопасности

владеть:

− навыками реализации требуемых политик безопасности средствами операционных систем

− оценки эффективности работы операционной системы и её подсистем обеспечения информационной безопасности

Процесс изучения дисциплины направлен на формирование следующих компетенций*:*

− способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК–7)

− способность администрировать подсистемы информационной безопасности объекта защиты (ПК-3);

− способность учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации (ПСК-4.1)

− способность выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей (ПСК-4.2).

2. Указание места дисциплины в структуре образовательной программы

Дисциплина относится к дисциплинам базовой части профессионального цикла (Б1.Б.33). Изучается на 3 курсе в 6 семестре

3. Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоёмкость (объём) дисциплины составляет 5 зачётных единиц, 180 часов

Таблица 3.1 – Объём дисциплины по видам учебных занятий

Общая трудоемкость дисциплины	180
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	90,15
лекции	36
лабораторные занятия	36
практические занятия	18
экзамен	0,15

зачет	
курсовая работа (проект)	
расчетно-графическая (контрольная) работа	
Аудиторная работа (всего):	90
в том числе:	
лекции	36
лабораторные занятия	36
практические занятия	18
Самостоятельная работа обучающихся (всего)	53,85
Контроль/экз (подготовка к экзамену)	36

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Содержание дисциплины

Таблица 4.1 – Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел (тема) дисциплины	Содержание
1.	Понятие ОС, история, классификация, основные функции.	Понятие операционной системы, история развития системного программного обеспечения, принципы функционирования операционных систем
2.	Процессы, модель, состояния.	Понятие процесса, контекст процесса, диспетчеризация процессов.
3.	Нити. Диспетчеризация и синхронизация процессов.	Понятие нити или потока управления. Алгоритмы диспетчеризации потоков управления
4.	Проблемы межпроцессного взаимодействия.	Гонки процессов. Понятие критической секции. Алгоритмы предотвращения гонок процессов. Семафоры
5.	Взаимоблокировки процессов	Понятие взаимоблокировки. Причины взаимоблокировок. Методы борьбы с взаимоблокировками. Алгоритмы обхода взаимоблокировок
6.	Управление памятью в ОС	Основные принципы организации подсистем управления памяти виртуальная память, подкачка на диск, методы организации виртуальной памяти. Кольцевая защита процессора.
7.	Файловые системы. Механизмы защиты	Назначение, классификация, принципы организации файловых систем. Учёт сводного дискового пространства, методы повышения надежности и быстродействия файловых систем.
8.	Управление вводом – выводом в ОС.	Использование архитектур, отличных от фоннеймановской. Системы перлюстрации запросов на обращения к данным. Защита от считывания со сменных носителей.

9.	Механизмы разграничения доступа в ОС	Организация, функции, компоненты, защитные механизмы современных операционных систем
10.	Механизмы безопасной работы в ОС	Принципы реализации политик безопасности в ОС. Мандатная, дискреционная и групповые политики. .
11.	Администрирование ОС	Принципы администрирования операционных систем семейства Linux и Windows. Команды управления полномочиями

Таблица 4.2 –Содержание дисциплины и её методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		лек., час	№ лб.	№ пр.			
1	2	3	4	5	6	7	8
1.	Понятие ОС, история, классификация, основные функции.	2			У-1	С,Т	ПК-3, ПСК-4.1, ПСК-4.2
2.	Процессы, модель, состояния.	2			У-1-3, 6	С,Т	ПК-3, ПСК-4.1, ПСК-4.2
3.	Нити. Диспетчеризация и синхронизация процессов.	4	1	1	У-1,4-6 МО-1,6	С	ПК-3, ПСК-4.1, ПСК-4.2
4.	Проблемы межпроцессного взаимодействия.	2		2	У-2,8 МО-7	С	ОПК-7, ПСК-4.1, ПСК-4.2
5.	Взаимоблокировки процессов	2		3	У-1,9-12 МО-8	С	ПК-3, ПСК-4.1, ПСК-4.2
6.	Управление памятью в ОС	6	2		У-1,4-6 МО-2	С ,Т	ОПК-7, ПСК-4.2
7.	Файловые системы. Механизмы защиты	4			У-1,8-10	С ,Т	ПК-3, ПСК-4.1, ПСК-4.2
8.	Управление вводом – выводом в ОС.	4			У-1,4-6	С	ПК-3, ПСК-4.1, ПСК-4.2
9.	Механизмы разграничения доступа в ОС	2	3		У-1,4-6 МО-3	С	ПК-3, ПСК-4.1, ПСК-4.2
10.	Механизмы безопасной работы в ОС	4	4		У-2,9-13 МО-4	С,Т	ПК-3, ПСК-4.1, ПСК-4.2
11.	Администрирование ОС	4	5		У-3,12 МО-5	С	ПК-3, ПСК-4.1, ПСК-4.2

С – собеседование, Т – тест

4.2. Лабораторные работы и практические занятия

4.2.1. Лабораторные работы

Таблица 4.3 – Лабораторные работы

№	Наименование лабораторной работы	Объем, час.
1.	Разработка многонитевой программы	6
2.	Исследование структуры файла	8
3.	Установка и администрирование операционной системы FreeBSD	8
4.	Настройка межсетевого экрана в Linux	8
5.	Настройка межсетевого экрана в операционной системе Windows	6
Итого		36

4.2.2. Практические занятия

Таблица 4.4 – Практические занятия

№	Наименование лабораторной работы	Объем, час.
1.	Моделирование доступа к разделяемому ресурсу	4
2.	Анализ обращений потоков к общему ресурсу	6
3.	Исследование тупиковых ситуаций	8
Итого		18

4.3. Самостоятельная работа студентов (СРС)

Таблица 4.5 – Самостоятельная работа студентов

№	Наименование раздела учебной дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1.	Понятие ОС, история, классификация, основные функции.	1-2 недели	4
2.	Процессы, модель, состояния.	2-3 недели	5
3.	Нити. Диспетчеризация и синхронизация процессов.	3-4 недели	3
4.	Проблемы межпроцессного взаимодействия.	5-6 недели	5
5.	Взаимоблокировки процессов	6-8 недели	9,85
6.	Управление памятью в ОС	8-9 недели	5
7.	Файловые системы. Механизмы защиты	9-10 недели	5
8.	Управление вводом – выводом в ОС.	11-12 недели	5
9.	Механизмы разграничения доступа в ОС	12-14 недели	5
10.	Механизмы безопасной работы в ОС	14-15 недели	2
11.	Администрирование ОС	15-18 недели	5
Итого			53,85

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное Правилами внутреннего распорядка работников.

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

− библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с данной РПД;

− имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

− путем обеспечения доступности всего необходимого учебно-методического и справочного материала;

− путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;

− путем разработки вопросов к экзамену, методических указаний к выполнению лабораторных и практических работ.

типографией университета:

− путем помощи авторам в подготовке и издании научной, учебной, учебно-методической литературы;

− путем удовлетворения потребностей в тиражировании научной, учебной, учебно-методической литературы.

6. Образовательные технологии

В соответствии с требованиями ФГОС и Приказа Министерства образования и науки РФ от 05 апреля 2017 г. №301 реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков студентов. Удельный вес занятий, проводимых в интерактивных формах, составляет 24.9% от аудиторных занятий согласно УП. Средствами промежуточного контроля успеваемости студентов являются защита лабораторных работ, опросы на практических занятиях по темам лекций.

Таблица 6.1 – Интерактивные образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела	Используемые интерактивные	Объём

		образовательные технологии	, час.
1.	Выполнение лабораторной работы №1 «Разработка многонитевой программы»	Исследование возможности передачи межпроцессных сообщений различными средствами	6
2.	Выполнение лабораторной работы №2 «Исследование структуры файла»	Выполнение студентом интерактивных заданий по определению основных элементов исполняемых файлов	8
3.	Выполнение лабораторной работы №3 «Установка и администрирование операционной системы FreeBSD»	Выполнение студентом интерактивных заданий по реализации требуемых политик безопасности	8
4.	Выполнение практической работы №2 «Анализ обращений потоков к общему ресурсу»	Исследование влияния интенсивности обращений к ресурсам со стороны процессов на частоту простоя и ожидания освобождения ресурсов	6
5.	Выполнение практической работы №3 «Исследование тупиковых ситуаций»	Составление и исследование студентами модели обращения процессов к счётному разделяемому ресурсу	8
	Итого		36

7. Фонд оценочных средств для проведения промежуточной аттестации

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

Таблица 7.1 – Этапы формирования компетенций

Код и содержание компетенции	Этапы формирования компетенций и дисциплины (модули), при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
ОПК-7 - способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Информационные технологии Практика по получению первичных профессиональных умений и навыков	Основы управления информационной безопасностью Безопасность операционных систем Безопасность сетей ЭВМ Технические средства охраны	Программно-аппаратные средства защиты информации Техническая защита информации Сети и системы передачи информации Администрирование вычислительных сетей Защита информационных

		Системы контроля доступа и видеонаблюдения	процессов в компьютерных системах Преддипломная практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты
способность администрировать подсистемы информационной безопасности объекта защиты (ПК-3)	Информационные технологии	Техническая защита информации; Безопасность операционных систем; Технические средства охраны; Системы контроля доступа и видеонаблюдения	Эксплуатационная практика; Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты
способностью учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации (ПСК-4.1)	Практика по получению первичных профессиональных умений и навыков	Безопасность операционных систем; Организация ЭВМ и вычислительных систем	Администрирование вычислительных сетей; Специализированные вычислительные устройства защиты информации; Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты

способностью выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей (ПСК-4.2)		Безопасность систем баз данных; Безопасность операционных систем	Администрирование вычислительных сетей; Сети и системы передачи информации (специальные разделы) Беспроводные сети связи; Эксплуатационная практика; Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты

7.2. Описание показателей и критериев оценивания компетенций на раз- личных этапах их формирования, описание шкал оценивания

Таблица 7.2 – Критерии и шкала оценивания компетенций

Наименование компетенции	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
ОПК - 7/ *основной*	*1.Доля освоенных обучающимся знаний, умений навыков от общего объема ЗУН, установленных в п.1.ЗРПД* *2.Качество освоенных обучающи-мися знаний, умений, навыков* *3. Умение*	**Знать**: -основные понятия курса. **Уметь**: - применять теоретические сведения при решении типовых задач. **Владеть**: - навыками анализа структуры систем по передаче	**Знать**: -основные характеристики сигналов; -основные протоколы взаимодействия компонентов операционных систем. **Уметь**: - применять знания о системах для решения задач	**Знать**: - характеристики операционных систем; - принципы построения и функционирования систем информации; - способы обработки информации в компьютерных системах; **Уметь**:

	применять знания, умения, навыки в типовых и нестандартных ситуациях	информации.	по созданию защищенных информационны х систем; **Владеть**: - навыками анализа основных характеристик операционных систем.	- применять знания о системах электрической связи для решения типовых и нестандартных задач по созданию защищенных операционных систем; - анализировать тенденции развития систем обеспечения информационной безопасности. **Владеть**: - навыками анализа характеристик и возможностей операционных систем по защищённой обработке данных.
способнос ть администр ировать подсистем ы информац ионной безопаснос ти объекта защиты (ПК-3)	1.Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.1.3 РПД 2.Качество освоенных обучающимся знаний, умений, навыков 3.Умение применять знания, умения, навыки в типовых и нестандартных ситуациях	**Знать**: функционал администратора безопасность ОС **Уметь**: выполнять администрирую щие инструкции в современных ОС **Владеть навыками**: эксплуатации различных компонентов подсистем обеспечения ИБ современных ОС	**Знать**: принципы организации подситем безопасности ОС **Уметь**: настраивать компонентов безопасности ОС **Владеть навыками**: администрирова ния компонентов безопасности ОС	**Знать**: критерии соответствия функционала подсистем информационной безопасности угрозам для объектов информатизации **Уметь**: выбирать требуемы политики безопасности при настройке безопасности ОС **Владеть навыками**: реагировании на нештатные ситуации, возникающие при эксплуатации компонентов безопасности ОС
способнос тью учитывать и использова	1.Доля освоенных обучающимся знаний, умений, навыков от	**Знать**: используемые в работе с ОС программные средства	**Знать**: инструментальн ые средства проведения проверок	**Знать**: основные угрозы работоспособности прогаммным компонентам СЗИ

ть особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации (ПСК-4.1)	общего объема ЗУН, установленных в п.1.3 РПД 2.Качество освоенных обучающимся знаний, умений, навыков 3.Умение применять знания, умения, навыки в типовых и нестандартных ситуациях	**Уметь**: использовать в работе с ОС программные средства разработки ПО и администрирования **Владеть навыками**: разработки ПО	информационных систем **Уметь**: анализ кода программных СЗИ **Владеть навыками**: риверс-инжиниринга программных средств	**Уметь**: выявлять недекларируемые возможности программных систем **Владеть навыками**: использования особенностей реализации ПО для обеспечения ИБ
способностью выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей (ПСК-4.2)	1.Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.1.3 РПД 2.Качество освоенных обучающимся знаний, умений, навыков 3.Умение применять знания, умения, навыки в типовых и нестандартных ситуациях	**Знать**: понятие политики безопасности и средства ОС, которыми она может быть реализована администрирующие инструкции в современных ОС **Владеть навыками**: эксплуатации различных компонентов подсистем обеспечения ИБ современных ОС	**Знать**: принципы организации подситем безопасности ОС **Уметь**: настраивать компонентов безопасности ОС **Владеть навыками**: администрирования компонентов безопасности ОС	**Знать**: критерии соответствия функционала подсистем информационной безопасности угрозам для объектов информатизации **Уметь**: выбирать требуемы политики безопасности при настройке безопасности ОС **Владеть навыками**: реагировании на нештатные ситуации, возникающие при эксплуатации компонентов безопасности ОС

7.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Таблица 7.3 – Паспорт комплекта оценочных средств для текущего контроля

п/п	Раздел (тема) дисциплины	Код контроли-руемой компе-тенции (или её части)	Технология формирова-ния	Оценочные средства		Описание шкал оценивания
				наимено вание	№№ заданий	
1	2	3	4	5	6	7
1.	Понятие ОС, история, классификация, основные функции.	ПК-3, ПСК-4.1, ПСК-4.2	Лекция, СРС	Собеседование, тест	1-25	Согласно табл.7.2
2.	Процессы, модель, состояния.	ПК-3, ПСК-4.1, ПСК-4.2	Лекция, СРС	Собеседование, тест	1-24	Согласно табл.7.2
3.	Нити. Диспетчеризация и синхронизация процессов.	ПК-3, ПСК-4.1, ПСК-4.2 ОПК-7	Лекция, СРС, лабораторная работа	собеседование		Согласно табл.7.2
				контрольные вопросы к ЛР№1		
				контрольные вопросы к ПР№1	1-5	
4.	Проблемы межпроцессного взаимодействия.	ОПК-7, ПСК-4.2 ПК-3, ПСК-4.1		собеседование		Согласно табл.7.2
				контрольные вопросы к ПР№2		
5.	Взаимоблокировки процессов	ПК-3, ПСК-4.1, ПСК-4.2		собеседование		Согласно табл.7.2

				контрольные вопросы к ПР№3	1-5	
6.	Управление памятью в ОС	ПК-3, ПСК-4.1, ПСК-4.2		Собеседование, тест	1-42	Согласно табл.7.2
				контрольные вопросы к ЛР№2		
7.	Файловые системы. Механизмы защиты	ПК-3, ПСК-4.1, ПСК-4.2		Собеседование, тест	1-16	Согласно табл.7.2
8.	Управление вводом – выводом в ОС.	ПК-3, ПСК-4.1, ПСК-4.2		собеседование		Согласно табл.7.2
9.	Механизмы разграничения доступа в ОС	ПК-3, ПСК-4.1, ПСК-4.2		собеседование		Согласно табл.7.2
				контрольные вопросы к ЛР№3	1-5	
10.	Механизмы безопасной работы в ОС	ПК-3, ПСК-4.1, ПСК-4.2 ОПК-7		Собеседование, тест	1-13	Согласно табл.7.2
				контрольные вопросы к ЛР№4	1-5	
11.	Администрирование ОС	ПК-3, ПСК-4.1, ПСК-4.2		собеседование		Согласно табл.7.2
				контрольные вопросы к ЛР№5	1-5	

Умения, навыки и компетенции проверяются с помощью задач (ситуационных, производственных или кейсового характера) и различного вида конструкторов. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

7.4. Рейтинговый контроль изучения учебной дисциплины

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

– Положение П 02.016–2018 «О балльно-рейтинговой системе оценивания результатов обучения по дисциплинам (модулям) и практикам при освоении обучающимися образовательных программ»;

– методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля* по дисциплине в рамках действующей в университете балльно-рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
Выполнение лабораторной работы №1 «Разработка многонитевой программы»	3	Выполнил, но «не защитил»	5	Выполнил и «защитил»
Выполнение лабораторной работы №2 «Исследование структуры файла»	3	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Выполнение лабораторной работы №3 «Установка и администрирование операционной системы	3	Выполнил, но «не защитил»	5	Выполнил и «защитил»
[illegible] лабораторной работы №4 «Настройка межсетевого экрана в Linux»	3	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Выполнение лабораторной работы №5 «Настройка межсетевого экрана в операционной системе Windows»	3	Выполнил, но «не защитил»	5	Выполнил и «защитил»
Выполнение практической работы №1 «Моделирование доступа к разделяемому ресурсу»	3	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Выполнение практической работы №2 «Анализ обращений потоков к общему ресурсу»	3	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Выполнение практической работы №3 «Исследование тупиковых ситуаций»	3	Выполнил, но «не защитил»	5	Выполнил и «защитил»
СРС	0		12	
ИТОГО	24		48	
Посещаемость	0		16	

Экзамен	0		36	
ИТОГО	24		100	

При итоговом контроле в форме бланкового теста студенту предлагается 15 вопросов по различным темам курса. Полученную итоговую сумму условных баллов (максимум 15) переводят в баллы на экзамене (максимум 36) путём умножения на 2.4 и округления до целого значения.

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

8.1. Основная литература

1) Операционные системы, среды и оболочки :[Текст] : учебное пособие / Т.Л. Партыка, И. И. Попов. – 4-е изд., перераб. И доп. – М.: ФОРУМ, 2012. – 560 с.: ил.

2) Операционные системы [Текст] : учебник / С. В. Синицын, А. В. Батаев, Н. Ю. Налютин. – 2-е изд., испр. – М.: Академия, 2012. – 304 с

3) Технические средства и методы защиты информации [Текст] : учебное пособие / под ред. А. П. Зайцева и А. А. Шелупанова. - М. : Горячая линия - Телеком, 2012. - 616 с.

8.2. Дополнительная литература

4) Организация ЭВМ и вычислительных систем [Текст] : учебник / Ю. Г. Древс. – М.: Высшая школа, 2006. – 501 с.: ил.

5) Сетевые операционные системы [Текст] / В.Г. Олифер, Н.А. Олифер – СПб.: Издательский дом «Питер», 2003.

6) Операционные системы [Текст] / В. П. Грибанов– М.: Издательский дом «Вильямс», 2002.

7) Системное программирование в Windows 2000 для профессионалов. [Текст] / А. Вильямс – СПб.: Издательский дом «Питер», 2001.

8) Операционные системы [Текст] : учебник / А.В. Гордеев – 2-е изд. – СПб. : Питер, 2009. – 416 с..

9) Микропроцессоры и операционные системы : Краткое справочное пособие [Текст] / Р . Холленд - М. : Энергоатомиздат, 1991.- 192 с.: ил.

10) Интернет: протоколы безопасности. учебный курс [Текст] / У. Блэк – СПб.: Издательский дом «Питер», 2001.

11) Системное программное обеспечение [Текст] / А.В. Гордеев, А.Ю. Молчанов.– Спб.: Питер, 2001. – 736с. Илл.

12) Введение в операционные системы [Текст] / Г. Дейтел– М.: «Мир», 1987.

13) Windows для профессионалов: создание эффективных WIN32 приложений с учетом специфики 64-х разрядной версии Windows. [Текст] / Дж. Рихтер– М.: Питер, 2001. – 752 с.

14) Операционная система UNIX. [Текст] / А. Робачевский– СПб.: «BHV-Петербург», 1999.

15) Системное программирование в UNIX. [Текст] / К. Хевиленд, Д. Грэй, Б.Салама – М.: «ДМК Пресс», 2000.

8.3. Перечень методических указаний

1) Разработка многонитевой программы : методические указания к лабораторной работе по дисциплине «Безопасность операционных систем» (учебно-методическая разработка) / М.О. Таныгин - Курск: Юго–Зап. Гос. Ун-т, 2017. 42 с.

2) Обзор PE-формата исполняемых файлов платформы Win32:методические указания к лабораторной работе по дисциплине «Безопасность операционных систем» (учебно-методическая разработка) / М.О. Таныгин - Курск: Юго–Зап. Гос. Ун-т, 2017. 20 с.

3) Установка и администрирование операционной системы FreeBSD: методические указания по выполнению лабораторной работы по дисциплине «Безопасность операционных систем» (учебно-методическая разработка) / М.О. Таныгин – Курск: Юго–Зап. Гос. Ун-т, 2016. 43 с.

4) Настройка межсетевого экрана в Linux :методические указания к лабораторной работе по дисциплине «Безопасность операционных систем» (учебно-методическая разработка) / М.О. Таныгин - Курск: Юго–Зап. Гос. Ун-т, 2017. 53 с.

5) Настройка межсетевого экрана в операционной системе Windows :методические указания по выполнению лабораторной работы по дисциплине «Безопасность операционных систем» (учебно-методическая разработка) / М.О. Таныгин – Курск: Юго–Зап. Гос. Ун-т, 2016. 19 с.

6) Моделирование доступа к разделяемому ресурсу :методические указания к практической работе по дисциплине «Безопасность операционных систем» (учебно-методическая разработка) / М.О. Таныгин - Курск: Юго–Зап. Гос. Ун-т, 2017. 18 с.

7) Анализ обращений потоков к общему ресурсу :методические указания по выполнению практической работы по дисциплине «Безопасность операционных систем» (учебно-методическая разработка) / М.О. Таныгин – Курск: Юго–Зап. Гос. Ун-т, 2017. 10 с.

8) Исследование тупиковых ситуаций: методические указания по выполнению практической работы по дисциплине «Безопасность операционных систем» (учебно-методическая разработка) / М.О. Таныгин – Курск: Юго–Зап. Гос. Ун-т, 2017. 17 с.

9. Перечень ресурсов информационно-телекоммуникационной сети Интернет

1) Федеральная служба безопасности [официальный сайт]. Режим доступа: http://www.fsb.ru/
2) Федеральная служба по техническому и экспортному контролю [официальный сайт]. Режим доступа: http://fstec.ru/

3) Сообщество Ubuntu [официальный сайт]. Режим доступа: http://ubuntu.com/
4) Корпорация Microsoft [официальный сайт]. Режим доступа: http://microsoft.com/
5) Электронно-библиотечная система «Университетская библиотека онлайн» Режим доступа: http://biblioclub.ru
6) Компания «Консультант Плюс» [официальный сайт]. Режим доступа: http://www.consultant.ru
7) Научно-информационный портал ВИНИТИ РАН [официальный сайт]. Режим доступа: http://www.consultant.ru/
8) База данных "Патенты России"

10. Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Безопасность операционных систем» являются лекции, практические и лабораторные занятия. Студент не имеет права пропускать занятия без уважительных причин.

На лекциях излагаются и разъясняются основные понятия темы, связанные с ней теоретические и практические проблемы, даются рекомендации для самостоятельной работы. В ходе лекции студент должен внимательно слушать и конспектировать материал.

Изучение наиболее важных тем или разделов дисциплины завершают лабораторные и практические занятия, которые обеспечивают: контроль подготовленности студента; за- крепление учебного материала; приобретение опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Лабораторному занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования, защиты отчетов по лабораторным и практическим работам.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Безопасность операционных систем»: конспектирование учебной литературы и лекции, составление словарей понятий и терминов и т. п.

В процессе обучения преподаватели используют активные формы работы со студентами: чтение лекций, привлечение студентов к творческому процессу на лекциях, промежуточный контроль путем отработки студентами пропущенных лекции, участие в групповых и индивидуальных консультациях (собеседовании). Эти формы способствуют выработке у

студентов умения работать с учебником и литературой. Изучение литературы и справочной документации составляет значительную часть самостоятельной работы студента. Это большой труд, требующий усилий и желания студента. В самом начале работы над книгой важно определить цель и направление этой работы. Прочитанное следует закрепить в памяти. Одним из приемов закрепление освоенного материала является конспектирование, без которого немыслима серьезная работа над литературой. Систематическое конспектирование помогает научиться правильно, кратко и четко излагать своими словами прочитанный материал.

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Безопасность операционных систем» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Безопасность операционных систем» - закрепить теоретические знания, полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

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

Microsoft Office 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №K0000000117 от 21.12.2015 г. с ООО «СМСКанал», Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234,Windows 7, договор IT000012385, Oracle Virtualbox (Бесплатная, GNU General Public License), редактор двоичных файлов Free Hex Editor Neo, (Свободное ПО http://www.hhdsoftware.com/free-hex-editor), открытая среда разработки программного обеспечения Lazarus (Свободное ПО http://www.lazarus.freepascal.org/) ОС FreBSD (свободное ПО, лицензия BSD), ОС Ubuntu (Бесплатная, GNU GPLv3)

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

Учебная аудитория для проведения занятий лекционного типа и лаборатории кафедры информационной безопасности, оснащенные учебной

мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска. Компьютеры (10 шт) CPU AMD-Phenom, ОЗУ 16 GB, HDD 2 Tb, монитор Aok 21”. Проекционный экран на штативе; Мультимедиацентр: ноут- букASUSX50VLPMD-T2330/14"/1024Mb/160Gb/сумка/ проектор inFocusIN24+