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

Кафедра вычислительной техники

“УТВЕРЖДАЮ”
ДЕКАН АВТФ
к.т.н. Рева И. Л.
“___”_____ _____ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Безопасность операционных систем

Образовательная программа: 10.05.03 Информационная безопасность автоматизированных систем, специализация: Информационная безопасность автоматизированных систем критически важных объектов

Курс: 3, семестр : 5

Факультет автоматики и вычислительной техники,

		Семестр
№	**Вид деятельности**	**5**
1	Всего зачетных единиц (кредитов)	3
2	Всего часов	108
3	Всего занятий в контактной форме, час.	45
4	Лекции, час.	18
5	Практические занятия, час.	0
6	Лабораторные занятия, час.	18
7	из них в активной и интерактивной форме, час.	18
8	Аттестация, час.	2
9	Консультации, час.	7
10	Самостоятельная работа, час.	63
11	Виды самостоятельной работы (курсовой проект, курсовая работа, РГЗ, подготовка к контрольной работе)	
12	Вид аттестации	Э

Новосибирск 2017

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования по направлению (специальности): 10.05.03 Информационная безопасность автоматизированных систем

ФГОС введен в действие приказом №1509 от 01.12.2016 г. , дата утверждения: 20.12.2016 г.

Место дисциплины в структуре учебного плана: Блок 1, базовая

Рабочая программа разработана на основе компетентностной модели выпускника по направлению (специальности): 10.05.03 Информационная безопасность автоматизированных систем

Рабочая программа обсуждена на заседании кафедры

ВТ, протокол заседания кафедры №6 от 20.06.2017

Утверждена на совете факультета автоматики и вычислительной техники, протокол № 6 от 21.06.2017

Программу разработал:

доцент, к.ф-м.н. Котов Ю. А.

Заведующий кафедрой:

доцент, к.т.н. Якименко А. А.

Ответственный за образовательную программу:

заведующий кафедрой Трушин В. А.

1. Внешние требования

Таблица 1.1

***Компетенция ФГОС*: ПК.11 способность разрабатывать политику информационной безопасности автоматизированной системы; *в части следующих результатов обучения*:**
з1. знать принципы формирования политики информационной безопасности в автоматизированных системах
у1. уметь реализовывать политику безопасности автоматизированной системы
***Компетенция ФГОС*: ПК.12 способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы; *в части следующих результатов обучения*:**
з2. знать методы управления информационной автоматизированной системой
у2. уметь управлять информационной безопасностью автоматизированной системы
у3. уметь разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы
***Компетенция ФГОС*: ПК.13 способность участвовать в проектировании средств защиты информации автоматизированной системы; *в части следующих результатов обучения*:**
у1. уметь проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы
***Компетенция ФГОС*: ПК.17 способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации; *в части следующих результатов обучения*:**
з1. знать методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем
з2. знать автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности
у2. уметь проводить инструментальный мониторинг защищенности автоматизированных систем
***Компетенция ФГОС*: ПК.19 способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы; *в части следующих результатов обучения*:**
у1. уметь администрировать подсистемы безопасности автоматизированных систем
***Компетенция ФГОС*: ПК.2 способность создавать и исследовать модели автоматизированных систем; *в части следующих результатов обучения*:**
у1. уметь подобрать составляющие элементы автоматизированной системы для реализации поставленных задач
у2. уметь сформировать требования к автоматизированной системе
***Компетенция ФГОС*: ПК.22 способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации; *в части следующих результатов обучения*:**
у1. уметь формировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе

2. Требования НГТУ к результатам освоения дисциплины

Таблица 2.1

Результаты изучения дисциплины по уровням освоения (иметь представление, знать, уметь, владеть)	**Формы организации занятий**
Безопасность операционных систем	
ПК.2.у1 уметь подобрать составляющие элементы автоматизированной системы для реализации поставленных задач	
1.уметь подобрать составляющие элементы автоматизированной системы для реализации поставленных задач	Лекции; Лабораторные работы; Самостоятельная работа
ПК.2.у2 уметь сформировать требования к автоматизированной системе	

2.уметь сформировать требования к автоматизированной системе	Лекции; Лабораторные работы; Самостоятельная работа
ПК.11.з1 знать принципы формирования политики информационной безопасности в автоматизированных системах	
3.знать принципы формирования политики информационной безопасности в автоматизированных системах	Лекции; Лабораторные работы; Самостоятельная работа
ПК.11.у1 уметь реализовывать политику безопасности автоматизированной системы	
4.уметь реализовывать политику безопасности автоматизированной системы	Лекции; Лабораторные работы; Самостоятельная работа
ПК.12.з2 знать методы управления информационной автоматизированной системой	
5.знать методы управления информационной автоматизированной системой	Лекции; Лабораторные работы; Самостоятельная работа
ПК.12.у2 уметь управлять информационной безопасностью автоматизированной системы	
6.уметь управлять информационной безопасностью автоматизированной системы	Лекции; Лабораторные работы; Самостоятельная работа
ПК.12.у3 уметь разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	
7.уметь разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	Лекции; Лабораторные работы; Самостоятельная работа
ПК.13.у1 уметь проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы	
8.уметь проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы	Лекции; Лабораторные работы; Самостоятельная работа
ПК.17.з1 знать методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем	
9.знать методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем	Лекции; Лабораторные работы; Самостоятельная работа
ПК.17.з2 знать автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности	
10.знать автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности	Лекции; Лабораторные работы; Самостоятельная работа
ПК.17.у2 уметь проводить инструментальный мониторинг защищенности автоматизированных систем	
11.уметь проводить инструментальный мониторинг защищенности автоматизированных систем	Лекции; Лабораторные работы; Самостоятельная работа
ПК.19.у1 уметь администрировать подсистемы безопасности автоматизированных систем	
12.уметь администрировать подсистемы безопасности автоматизированных систем	Лекции; Лабораторные работы; Самостоятельная работа
ПК.22.у1 уметь формировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе	
13.уметь формировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе	Лекции; Лабораторные работы; Самостоятельная работа

3. Содержание и структура учебной дисциплины

Таблица 3.1

Темы лекций	Активные формы, час.	Часы	Ссылки на результаты обучения
Семестр: 5			
Дидактическая единица: Безопасность операционных систем			
1. Назначение и задачи операционных систем. Архитектура ОС. Классификация ОС	0	1	1, 10, 11, 12, 13, 2, 3, 4, 5, 6, 7, 8, 9
2. Основные принципы построения и состав ОС. Начальная загрузка ОС. Интерфейсы ОС	0	2	1, 10, 11, 12, 13, 2, 3, 4, 5, 6, 7, 8, 9
3. Понятие процесса и его применение в ОС. Система прерываний в ОС Ресурсы ОС	0	1	1, 10, 11, 12, 13, 2, 3, 4, 5, 6, 7, 8, 9
4. Управление заданиями на уровне внешнего планирования в ОС. Алгоритмы внутреннего планирования в ОС	0	2	1, 10, 11, 12, 13, 2, 3, 4, 5, 6, 7, 8, 9
5. Параллельные процессы, критические ресурсы и участки. Понятие тупика. Алгоритмы предотвращения и обхода тупиков	0	2	1, 10, 11, 12, 13, 2, 3, 4, 5, 6, 7, 8, 9
6. Организация памяти в ОС. Принцип локальности	0	2	1, 10, 11, 12, 13, 2, 3, 4, 5, 6, 7, 8, 9
7. Организация данных в ОС. Организация файлов в ОС. Файловая система. Многоуровневая модель. Архитектура файловых систем	0	2	1, 10, 11, 12, 13, 2, 3, 4, 5, 6, 7, 8, 9
8. Элементы безопасности ОС Windows NT. Элементы безопасности ОС UNIX	0	2	1, 10, 11, 12, 13, 2, 3, 4, 5, 6, 7, 8, 9
9. Предмет и задачи защиты информации. Основные виды угроз и методы защиты информации	0	2	1, 10, 11, 12, 13, 2, 3, 4, 5, 6, 7, 8, 9
10. Криптографическая защита информации. Классификация шифров	0	2	1, 10, 11, 12, 13, 2, 3, 4, 5, 6, 7, 8, 9

Таблица 3.2

Темы лабораторных работ	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 5				
Дидактическая единица: Безопасность операционных систем				
11. Подсистема защиты ОС Windows	4	4	1, 10, 11, 12, 13, 2, 3, 4, 5, 6, 7, 8, 9	Подсистема защиты ОС Windows
12. Защита ОС и оболочка Windows Script	4	4	1, 10, 11, 12, 13, 2, 3, 4, 5, 6, 7, 8, 9	Защита ОС и оболочка Windows Script
13. Криптографическая защита и аутентификация	4	4	1, 10, 11, 12, 13, 2, 3, 4, 5, 6, 7, 8, 9	Криптографическая защита и аутентификация
14. Администрирование защиты в условиях дискреционного доступа	6	6	1, 10, 11, 12, 13, 2, 3, 4, 5, 6, 7, 8, 9	Администрирование защиты в условиях дискреционного доступа

4. Самостоятельная работа обучающегося

№	Виды самостоятельной работы	Ссылки на результаты обучения	Часы на выполнение	Часы на консультации
Семестр: 5				
1	Подготовка к занятиям	1, 10, 11, 12, 13, 2, 3, 4, 5, 6, 7, 8, 9	41	3
: Методы и средства защиты компьютерной информации. Ч. 1 : методические указания к лабораторным работам для 4 курса АВТФ / Новосиб. гос. техн. ун-т ; [сост. Ю. А. Котов]. - Новосибирск, 2010. - 35, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000146768				
2	Подготовка к аттестации	1, 10, 11, 12, 13, 2, 3, 4, 5, 6, 7, 8, 9	22	4
Подготока к аттестации: Методы и средства защиты компьютерной информации. Ч. 1 : методические указания к лабораторным работам для 4 курса АВТФ / Новосиб. гос. техн. ун-т ; [сост. Ю. А. Котов]. - Новосибирск, 2010. - 35, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000146768				

5. Технология обучения

Для организации и контроля самостоятельной работы обучающихся, а также проведения консультаций применяются информационно-коммуникационные технологии (табл. 5.1).

Таблица 5.1

Деятельность	Информационно-коммуникационные технологии
Информирование	e-mail
Консультирование	e-mail

6. Правила аттестации обучающихся по учебной дисциплине

Для аттестации обучающихся по дисциплине используется балльно-рейтинговая система (БРС), позволяющая выставлять оценки по традиционной шкале и 15-уровневой ECTS. Краткая информация о БРС приведена в табл. 6.1.

Таблица 6.1

Оцениваемые виды деятельности обучающихся	Максимальный балл
Семестр: 5	
Лабораторная:	40
Контролирующие материалы приводятся в "Методы и средства защиты компьютерной информации. Ч. 1 : методические указания к лабораторным работам для 4 курса АВТФ / Новосиб. гос. техн. ун-т ; [сост. Ю. А. Котов]. - Новосибирск, 2010. - 35, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000146768"	
РГЗ:	40
Контролирующие материалы приводятся в "Методы и средства защиты компьютерной информации. Ч. 1 : методические указания к лабораторным работам для 4 курса АВТФ / Новосиб. гос. техн. ун-т ; [сост. Ю. А. Котов]. - Новосибирск, 2010. - 35, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000146768"	
Зачет:	20
Контролирующие материалы приводятся в "Методы и средства защиты компьютерной информации. Ч. 1 : методические указания к лабораторным работам для 4 курса АВТФ / Новосиб. гос. техн. ун-т ; [сост. Ю. А. Котов]. - Новосибирск, 2010. - 35, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000146768"	

В таблице 6.2 представлено соответствие форм контроля заявляемым требованиям к результатам освоения дисциплины.

Таблица 6.2

Коды компетенций ФГОС	Результаты обучения	Формы контроля
		Защита Л/Р
ПК.11	з1. знать принципы формирования политики информационной безопасности в автоматизированных системах	+
	у1. уметь реализовывать политику безопасности автоматизированной системы	+
ПК.12	з2. знать методы управления информационной автоматизированной системой	+
	у2. уметь управлять информационной безопасностью автоматизированной системы	+
	у3. уметь разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	+
ПК.13	у1. уметь проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы	+
ПК.17	з1. знать методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем	+
	з2. знать автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности	+
	у2. уметь проводить инструментальный мониторинг защищенности автоматизированных систем	+
ПК.19	у1. уметь администрировать подсистемы безопасности автоматизированных систем	+
ПК.2	у1. уметь подобрать составляющие элементы автоматизированной системы для реализации поставленных задач	+
	у2. уметь сформировать требования к автоматизированной системе	+
ПК.22	у1. уметь формировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе	+

Фонд оценочных средств по дисциплине представлен в приложении № 1 к рабочей программе.

7. Литература

Основная литература

1. Вихман В. В. Методы и средства защиты компьютерной информации [Электронный ресурс] : электронный учебно-методический комплекс / В. В. Вихман ; Новосиб. гос. техн. ун-т. - Новосибирск, [2011]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000156312. - Загл. с экрана.

Дополнительная литература

1. Раводин О. М. Безопасность операционных систем : учебное пособие / О. М. Раводин, В. О. Раводин ; Томский гос. ун-т систем управления и радиоэлектроники. - Томск, 2005. - 226 с. : ил.

Интернет-ресурсы

1. ЭБС НГТУ : http://elibrary.nstu.ru/

2. ЭБС «Издательство Лань» : https://e.lanbook.com/

3. ЭБС IPRbooks : http://www.iprbookshop.ru/

4. ЭБС "Znanium.com" : http://znanium.com/

5. :

8. Методическое и программное обеспечение

8.1 Методическое обеспечение

1. Методы и средства защиты компьютерной информации. Ч. 1 : методические указания к лабораторным работам для 4 курса АВТФ / Новосиб. гос. техн. ун-т ; [сост. Ю. А. Котов]. - Новосибирск, 2010. - 35, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000146768

8.2 Специализированное программное обеспечение

1 Windows
2 Office

9. Материально-техническое обеспечение

Презентационное оборудование

№	Наименование	Назначение
1	Презентационное оборудование (мультимедиа-проектор, экран, компьютер для управления)	Применяется при проведении лекций

Компьютерный класс

№	Наименование	Назначение
1	Компьютерный класс (Компьютеры объединены в локальную сеть с выходом в Internet)	Применяется при проведении лабораторных занятий

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

Кафедра вычислительной техники

“УТВЕРЖДАЮ”
ДЕКАН АВТФ
к.т.н., доцент И.Л. Рева
“___”_____ _____ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

УЧЕБНОЙ ДИСЦИПЛИНЫ

Безопасность операционных систем

Образовательная программа: 10.05.03 Информационная безопасность автоматизированных систем, специализация: Информационная безопасность автоматизированных систем критически важных объектов

Новосибирск 2017

1. **Обобщенная структура фонда оценочных средств учебной дисциплины**

Обобщенная структура фонда оценочных средств по дисциплине Безопасность операционных систем приведена в Таблице.

Таблица

Формируемые компетенции	Показатели сформированности компетенций (знания, умения, навыки)	Темы	Этапы оценки компетенций	
			Мероприятия текущего контроля (курсовой проект, РГЗ(Р) и др.)	Промежуточная аттестация (экзамен, зачет)
ПК.1/Э способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	з3. знать программные и аппаратные средства защиты информации для типовых операционных систем, систем управления базами данных, компьютерных сетей	Предмет и задачи защиты информации. Основные виды угроз и методы защиты информации Администрирование защиты в условиях дискреционного доступа Защита ОС и оболочка Windows Script Криптографическая защита и аутентификация Криптографическая защита информации. Классификация шифров Назначение и задачи операционных систем. Архитектура ОС. Классификация ОС Организация данных в ОС. Организация файлов в ОС. Файловая система. Многоуровневая модель. Архитектура файловых систем Организация памяти в ОС. Принцип локальности Основные принципы построения и состав ОС. Начальная загрузка ОС. Интерфейсы ОС Параллельные процессы, критические ресурсы и участки. Понятие тупика. Алгоритмы предотвращения и обхода тупиков Подсистема защиты ОС Windows Понятие процесса и его применение в ОС. Система прерываний в ОС Ресурсы ОС Управление заданиями на уровне внешнего планирования в ОС. Алгоритмы внутреннего планирования в ОС Элементы безопасности ОС Windows NT. Элементы безопасности ОС UNIX	Контрольныя работа Отчет по лабораторной работе РГЗ, разделы 1-5	Зачет, вопросы 1-10
ПК.2/Э способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы	у2. уметь выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах	Предмет и задачи защиты информации. Основные виды угроз и методы защиты информации Администрирование защиты в условиях дискреционного доступа Защита ОС и оболочка Windows Script Криптографическая защита и аутентификация Криптографическая защита	Контрольная работы Отчет по лабораторной работе РГЗ, разделы 1-5	Зачет, вопросы 11-20

программирования для решения профессиональных задач		информации. Классификация шифров Назначение и задачи операционных систем. Архитектура ОС. Классификация ОС Организация данных в ОС. Организация файлов в ОС. Файловая система. Многоуровневая модель. Архитектура файловых систем Организация памяти в ОС. Принцип локальности Основные принципы построения и состав ОС. Начальная загрузка ОС. Интерфейсы ОС Параллельные процессы, критические ресурсы и участки. Понятие тупика. Алгоритмы предотвращения и обхода тупиков Подсистема защиты ОС Windows Понятие процесса и его применение в ОС. Система прерываний в ОС Ресурсы ОС Управление заданиями на уровне внешнего планирования в ОС. Алгоритмы внутреннего планирования в ОС Элементы безопасности ОС Windows NT. Элементы безопасности ОС UNIX		
ПК.3/Э способность администрировать подсистемы информационной безопасности объекта защиты	у3. уметь формировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе	Предмет и задачи защиты информации. Основные виды угроз и методы защиты информации Администрирование защиты в условиях дискреционного доступа Защита ОС и оболочка Windows Script Криптографическая защита и аутентификация Криптографическая защита информации. Классификация шифров Назначение и задачи операционных систем. Архитектура ОС. Классификация ОС Организация данных в ОС. Организация файлов в ОС. Файловая система. Многоуровневая модель. Архитектура файловых систем Организация памяти в ОС. Принцип локальности Основные принципы построения и состав ОС. Начальная загрузка ОС. Интерфейсы ОС Параллельные процессы, критические ресурсы и участки. Понятие тупика. Алгоритмы предотвращения и обхода тупиков Подсистема защиты ОС Windows Понятие процесса и его применение в ОС. Система прерываний в ОС Ресурсы ОС Управление	Контрольная работа Отчет по лабораторной работе РГЗ, разделы 1-5	Зачет, вопросы 20-40

		заданиями на уровне внешнего планирования в ОС. Алгоритмы внутреннего планирования в ОС Элементы безопасности ОС Windows NT. Элементы безопасности ОС UNIX		

В разделе 2 необходимо дать краткую характеристику мероприятиям текущего и промежуточного контроля, применяемым для оценки компетенций в рамках дисциплины. Далее в ФОС по дисциплине должны быть приведены паспорта тех мероприятий текущего и промежуточного контроля, которые указаны в последних столбцах таблицы с обобщенной структурой ФОС. Если дисциплина многосеместровая, то паспорта должны быть для всех видов промежуточной и текущей аттестации в каждом семестре.

2. Методика оценки этапов формирования компетенций в рамках дисциплины.

Промежуточная аттестация по дисциплине проводится в 4 семестре - в форме дифференцированного зачета, который направлен на оценку сформированности компетенций ПК.1/Э, ПК.2/Э, ПК.3/Э.

Зачет проводится в устной форме по билетам

Кроме того, сформированность компетенций проверяется при проведении мероприятий текущего контроля, указанных в таблице раздела 1.

В 4 семестре обязательным этапом текущей аттестации являются расчетно-графическое задание (работа) (РГЗ(Р)), контрольная работа. Требования к выполнению РГЗ(Р), контрольной работы, состав и правила оценки сформулированы в паспорте РГЗ(Р), контрольной работы.

Общие правила выставления оценки по дисциплине определяются балльно-рейтинговой системой, приведенной в рабочей программе дисциплины.

На основании приведенных далее критериев можно сделать общий вывод о сформированности компетенций ПК.1/Э, ПК.2/Э, ПК.3/Э, за которые отвечает дисциплина, на разных уровнях.

Общая характеристика уровней освоения компетенций.

Ниже порогового. Уровень выполнения работ не отвечает большинству основных требований, теоретическое содержание курса освоено частично, пробелы могут носить существенный характер, необходимые практические навыки работы с освоенным материалом сформированы не достаточно, большинство предусмотренных программой обучения учебных заданий не выполнены или выполнены с существенными ошибками.

Пороговый. Уровень выполнения работ отвечает большинству основных требований, теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые виды заданий выполнены с ошибками.

Базовый. Уровень выполнения работ отвечает всем основным требованиям, теоретическое содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые из выполненных заданий, возможно, содержат ошибки.

Продвинутый. Уровень выполнения работ отвечает всем требованиям, теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному.

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»
Кафедра вычислительной техники

Паспорт экзамена

по дисциплине «Безопасность операционных систем», 5 семестр

1. Методика оценки

Экзамен проводится в устной форме, по билетам. Билет формируется по следующему правилу: первый вопрос выбирается из диапазона вопросов 1-20, второй вопрос из диапазона вопросов 21-40 (список вопросов приведен ниже). В ходе экзамена преподаватель вправе задавать студенту дополнительные вопросы из общего перечня (п. 4).

Форма экзаменационного билета

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Факультет АВТФ

Билет № _____
к экзамену по дисциплине «Безопасность операционных систем»

---

1. Классификация ОС.
2. Шифры перестановки..

Утверждаю: зав. кафедрой ____ _____ должность, ФИО
(подпись)
(дата)

2. Критерии оценки

- Ответ на экзаменационный билет считается **неудовлетворительным**, если студент при ответе на вопросы не дает определений основных понятий, не способен показать причинно-следственные связи явлений, при решении задачи допускает принципиальные ошибки, оценка составляет *_10_ баллов.*
- Ответ на экзаменационный билет засчитывается на **пороговом** уровне, если студент при ответе на вопросы дает определение основных понятий, может показать причинно-следственные связи явлений, при решении задачи допускает непринципиальные

ошибки, например, вычислительные, оценка составляет *20 баллов.*

- Ответ на экзаменационный билет билет засчитывается на **базовом** уровне, если студент при ответе на вопросы формулирует основные понятия, законы, дает характеристику процессов, явлений, проводит анализ причин, условий, может представить качественные характеристики процессов, не допускает ошибок при решении задачи, оценка составляет *_30_ баллов.*
- Ответ на экзаменационный билет билет засчитывается на **продвинутом** уровне, если студент при ответе на вопросы проводит сравнительный анализ подходов, проводит комплексный анализ, выявляет проблемы, предлагает механизмы решения, способен представить количественные характеристики определенных процессов, приводит конкретные примеры из практики, не допускает ошибок и способен обосновать выбор метода решения задачи, оценка составляет _40_ *баллов.*

3. Шкала оценки

В общей оценке по дисциплине экзаменационные баллы учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

4. **Вопросы к** экзамену **по дисциплине «**Безопасность операционных систем**»**

1. Назначение и задачи операционных систем (ОС).
2. Классификация ОС.
3. Основные принципы построения и состав ОС.
4. Начальная загрузка ОС.
5. Интерфейсы ОС.
6. Понятие процесса и его применение в ОС.
7. Система прерываний в ОС.
8. Ресурсы ОС.
9. Управление заданиями на уровне внешнего планирования в ОС.
10. Алгоритмы внутреннего планирования в ОС.
11. Параллельные процессы, критические ресурсы и участки.
12. Понятие тупика. Алгоритмы предотвращения и обхода тупиков.
13. Организация памяти в ОС,
14. Принцип локальности.
15. Организация данных в ОС.
16. Организация файлов в ОС.
17. Файловая система. Многоуровневая модель.
18. Архитектура файловых систем.
19. Элементы безопасности ОС Windows NT.
20. Элементы безопасности ОС UNIX.

21. Предмет и задачи защиты информации.
22. Основные виды угроз и методы защиты информации.
23. Криптографическая защита информации. Классификация шифров.
24. Шифры замены.
25. Шифры перестановки.
26. Шифр гаммирования.

27. Шифр DES.
28. Шифр ГОСТ.
29. Криптосистемы с открытым ключем. Принцип Шеннона. Основные особенности и характеристики.
30. Шифр RSA.
31. Шифр Эль Гаммаля.
32. Основные проблемы криптографической защиты и способы их решения.
33. Методы идентификации/аутентификации, назначение и особенности.
34. Стандартные методы идентификации и аутентификации.
35. Доказательство с нулевой передачей знаний.
36. Электронная цифровая подпись.
37. Антивирусные программы и межсетевые экраны.
38. Методы доступа – основные виды и способы реализации.
39. Протоколирование и аудит.
40. Меры защищенности информационных систем.