МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНОБРНАУКИ РОССИИ)

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ДОНБАССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ДонГТУ»)

Факультет информационных технологий и автоматизации производственных процессов

Кафедра интеллектуальных систем и информационной безопасности

УТВЕРЖДАЮ
И.о. проректора
по учебной работе
Д.В. Мулов

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Безопасность операционных систем
(наименование дисциплины)

10.05.03 Информационная безопасность автоматизированных систем
(код, наименование специальности)

Безопасность открытых информационных систем
(специализация)

Квалификация специалист по защите информации
(бакалавр/специалист/магистр)

Форма обучения очная
(очная, очно-заочная, заочная)

Алчевск, 2024

1 Цели и задачи изучения дисциплины

Цели дисциплины. Целью изучения дисциплины «Безопасность операционных систем» является формирование у студентов теоретических знаний в области безопасности операционных систем, а также навыков практического применения полученных знаний.

Задачи изучения дисциплины. Привитие обучающимся основ культуры обеспечения информационной безопасности операционных систем, изучение таких разделов как основные понятия безопасности операционных систем, управления доступом, идентификация и аутентификация пользователей, аудит системы защиты, требования к защите информации операционных систем.

Дисциплина направлена на формирование общепрофессиональной (ОПК-12) компетенции выпускника.

2 Место дисциплины в структуре образовательной программы

Логико-структурный анализ дисциплины – курс входит в обязательную часть БЛОКА 1 «Дисциплины (модули)» подготовки студентов по специальности 10.05.03 Информационная безопасность автоматизированных систем (10.05.03-05 Безопасность открытых информационных систем).

Дисциплина реализуется кафедрой интеллектуальных систем и информационной безопасности. Основывается на базе дисциплин: «Информатика», «Физические основы построения технических средств защиты информации», «Теория информации», «Архитектура вычислительных систем», «Операционные системы».

Является основой для изучения следующих дисциплин: «Преддипломная практика», выполнение выпускной квалификационной работы, подготовка к процедуре защиты и защита выпускной квалификационной работы.

Для изучения дисциплины необходимы компетенции, сформированные у студента для решения профессиональных задач деятельности, в области операционных систем.

Курс является фундаментом для ориентации студентов в сфере разработки безопасных информационных систем.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единиц, 144 ак.ч. Программой дисциплины предусмотрены лекционные (36 ак.ч.), лабораторные (36 ак.ч.) занятия, самостоятельная работа студента (72 ак.ч.).

Дисциплина изучается на 3 курсе в 6 семестре. Форма промежуточной аттестации – экзамен.

3 Перечень результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины «Безопасность операционных систем» направлен на формирование компетенции, представленной в таблице 1.

Таблица 1 – Компетенции, обязательные к освоению

Содержание компетенции	Код компетенции	Код и наименование индикатора достижения компетенции
Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем	ОПК-12	ОПК-12.2 Применяет знания в области безопасности операционных систем при разработке автоматизированных систем

4 Объём и виды занятий по дисциплине

Общая трудоёмкость учебной дисциплины составляет 4 зачётных единицы, 144 ак.ч.

Самостоятельная работа студента (СРС) включает проработку материалов лекций, подготовку к практическим занятиям, текущему контролю, выполнение индивидуального задания, самостоятельное изучение материала и подготовку к экзамену.

При организации внеаудиторной самостоятельной работы по данной дисциплине используются формы и распределение бюджета времени на СРС для очной формы обучения в соответствии с таблицей 2.

Таблица 2 – Распределение бюджета времени на СРС

Вид учебной работы	Всего ак.ч.	Ак.ч. по семестрам
		6
Аудиторная работа, в том числе:	72	72
Лекции (Л)	36	36
Практические занятия (ПЗ)	-	-
Лабораторные работы (ЛР)	36	36
Курсовая работа/курсовой проект	-	-
Самостоятельная работа студентов (СРС), в том числе:	72	72
Подготовка к лекциям	9	9
Подготовка к лабораторным работам	10	10
Подготовка к практическим занятиям / семинарам	-	-
Выполнение курсовой работы / проекта	-	-
Расчетно-графическая работа (РГР)	-	-
Реферат (индивидуальное задание)	-	-
Домашнее задание	-	-
Подготовка к контрольным работам	-	-
Подготовка к коллоквиуму	-	-
Аналитический информационный поиск	9	9
Работа в библиотеке	8	8
Подготовка к экзамену	36	36
Промежуточная аттестация – экзамен (Э)	Э	Э
Общая трудоемкость дисциплины		
ак.ч.	144	144
з.е.	4	4

5 Содержание дисциплины

С целью освоения компетенций, приведенных в п.3 дисциплина разбита на 5 тем:

– тема 1 (Общие сведения о безопасности операционных систем);

– тема 2 (Способы и средств контроля доступа);

– тема 3 (Идентификация и аутентификация пользователей);

– тема 4 (Выявление вторжений. Аудит системы защиты);

– тема 5(Анализ некоторых популярных ОС с точки зрения их защищенности).

Виды занятий по дисциплине и распределение аудиторных часов для очной формы приведены в таблице 3.

Таблица 3 – Виды занятий по дисциплине и распределение аудиторных часов (очная форма обучения)

№ п/п	Наименование темы (раздела) дисциплины	Содержание лекционных занятий	Трудоемкость в ак.ч.	Темы практических занятий	Трудоемкость в ак.ч.	Тема лабораторных занятий	Трудоемкость в ак.ч.
1	2	3	4	5	6	7	8
1	Общие сведения о безопасности операционных систем	Требования к защите ОС. Угрозы безопасности. Методы обеспечения информационной безопасности. Модели безопасности ОС.	8	-	-	Средства межпроцессного взаимодействия	6
2	Способы и средств контроля доступа	Разграничение доступа в ОС. Авторизация. Способы управления доступом	6	-	-	Использование средств контроля доступа	6
3	Идентификация и аутентификация пользователей	Идентификация и аутентификация пользователей в ОС. Аутентификация по ключам, паролям и атрибутам пользователя	8	-	-	Права доступа	8
4	Выявление вторжений. Аудит системы защиты	Аудит в ОС. Выявление вторжений. Протоколирование. Функциональные компоненты и архитектура активного аудита	6	-	-	Выявление вторжений. Аудит системы защиты	8

Завершение таблицы 3

1	2	3	4	5	6	7	8
5	Анализ некоторых популярных ОС с точки зрения их защищенности	Программно-технический уровень информационной безопасности. Требования к защите компьютерной информации. Классификация требований к системе защиты. Различия требований и основополагающих механизмов защиты от несанкционированного доступа	8	-	-	Анализ некоторых популярных ОС с точки зрения их защищенности	8
Всего аудиторных часов		36		-		36	

6 Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине

6.1 Критерии оценивания

В соответствии с Положением о кредитно-модульной системе организации образовательного процесса ФГБОУ ВО «ДонГТУ» (https://www.dstu.education/images/structure/license_certificate/polog_kred_modul.pdf) при оценивании сформированности компетенций по дисциплине используется 100-балльная шкала.

Перечень компетенций по дисциплине и способы оценивания знаний приведены в таблице 4.

Таблица 4 – Перечень компетенций по дисциплине и способы оценивания знаний

Код и наименование компетенции	Способ оценивания	Оценочное средство
ОПК-9, ОПК-12	экзамен	Комплект контролирующих материалов для экзамена

Всего по текущей работе студент может набрать 100 баллов, в том числе:

– лабораторные работы – всего 100 баллов.

Оценка по экзамену проставляется автоматически, если студент набрал в течении семестра не менее 60 баллов и отчитался за каждую контрольную точку. Минимальное количество баллов по каждому из видов текущей работы составляет 60% от максимального.

Экзамен по дисциплине «Безопасность операционных систем» проводится по результатам работы в семестре. В случае, если полученная в семестре сумма баллов не устраивает студента, во время сессии студент имеет право повысить итоговую оценку либо в форме устного собеседования по приведенным ниже вопросам (п.п. 6.5), либо в результате тестирования.

Шкала оценивания знаний при проведении промежуточной аттестации приведена в таблице 5.

Таблица 5 – Шкала оценивания знаний

Сумма баллов за все виды учебной деятельности	Оценка по национальной шкале зачёт/экзамен
0-59	Не зачтено/неудовлетворительно
60-73	Зачтено/удовлетворительно
74-89	Зачтено/хорошо
90-100	Зачтено/отлично

6.2 Домашнее задание

Домашнее задание не предусмотрено.

6.3 Расчетно-графическая работа (РГР) – индивидуальное задание

Расчетно-графическая работа не предусмотрена.

6.4 Оценочные средства для самостоятельной работы и текущего контроля успеваемости

Тема 1 (Общие сведения о безопасности операционных систем)

1) Какие требования предъявляются к защите ОС?
2) Какие угрозы безопасности Вы знаете?
3) Какие методы обеспечения информационной безопасности Вы знаете?
4) Какие бывают модели безопасности ОС?
5) Что такое безопасность операционных систем?

Тема 2 (Способы и средств контроля доступа)

1) Что такое разграничение доступа в ОС?
2) Как производится разграничение доступа в ОС?
3) Что такое авторизация в ОС?
4) Как производится авторизация в ОС?
5) Какие бывают способы управления доступом?

Тема 3 (Идентификация и аутентификация пользователей)

1) Что такое идентификация пользователей в ОС?
2) Что такое аутентификация пользователей в ОС?
3) Чем отличается идентификация от аутентификации пользователей в ОС?
4) Как осуществляется аутентификация пользователя по ключам?
5) Как осуществляется аутентификация пользователя по паролям и атрибутам?

Тема 4 (Выявление вторжений. Аудит системы защиты)

1) Как осуществляется аудит в ОС?

2) Как осуществляется выявление вторжений?

3) Что такое протоколирование?

4) Что представляют из себя функциональные компоненты активного аудита?

5) Какова архитектура активного аудита?

Тема 5(Анализ некоторых популярных ОС с точки зрения их защищенности)

1) Что из себя представляет программно-технический уровень информационной безопасности?

2) Какие требования предъявляются к защите компьютерной информации?

3) Как можно классифицировать требования к системе защиты?

4) В чем состоят различия требований и основополагающих механизмов защиты от несанкционированного доступа?

5) Какие ОС, по Вашему мнению, наиболее защищены?

6.5 Вопросы для подготовки к экзамену

1) Что понимается под системой безопасности?

2) Какие вопросы, касающиеся информационной безопасности, содержатся в Конституции РФ?

3) Что такое операционная система?

4) Какие структурные компоненты операционных систем Вы знаете?

5) Какими основными дефектами обладают операционные системы с точки зрения обеспечения безопасности данных?

6) Какие существуют способы реализации защиты операционных систем?

7) Для чего необходимы средства профилактического контроля безопасности операционные системы?

8) Что представляет собой и для чего применяется матрица доступа?

9) Что представляют собой и для чего применяются списки доступа?

10) В чем заключаются самые значительные улучшения безопасности в Windows 11?

11) Какие требования предъявляются к параметрам пароля для ОС Linux?

12) Как в ОС Linux отключить доступ к консольным программам?

13) Какие дополнительные функции обеспечения информационной безопасности появились в Internet Explorer 8?

14) В чем состоят противоречия между реализованными в ОС механизмами защиты и принятыми формализованными требованиями?

15) В чем, с точки зрения обеспечения информационной безопасности, состоит отличие между централизованной и распределенной схемой администрирования?

16) Как реализуется структура прав доступа к файлу в системе Unix?

17) Какие уровни доступа реализованы на уровне файловой системы в UNIX?

18) Какие основные защитные механизмы реализованы в системе Unix?

19) Каковы основные недостатки защитных механизмов ОС семейства Unix?

20) Какие основные защитные механизмы реализованы в ОС семейства Windows NT?

21) Какие основные функции управления учетными записями пользователей реализованы в ОС семейства Windows NT?

22) Для чего предназначена служба Active Directory и какие она предоставляет возможности администрирования?

23) Каким образом система Kerberos реализует попарную проверку подлинности субъектов?

24) Какие выделяют группы методов, позволяющие несанкционированно вмешаться в работу системы?

25) Какие основные недостатки механизма защиты ОС используют средства несанкционированного доступа?

26) Какие существуют потенциальные опасности для базы данных?

27) В чем заключается утрата конфиденциальности данных?

28) Что понимается под угрозой базе данных?

29) Чем отличаются преднамеренные и не преднамеренные угрозы базе данных?

30) В чем состоит цель защиты базы данных?

31) Какие существуют аппаратные средства защиты базы данных?

32) Какие существуют программные средства защиты базы данных?

33) В чем заключается применение технологии RAID массивов?

34) Какие существуют уровни RAID массивов?

35) Как осуществляется защита СУБД в Web?

36) Какие возможности по защите баз данных предоставляют брандмауэры?

37) Какие основные механизмы защиты доступа к данным реализованы в СУБД?

38) Какие выделяют категории целостности данных?

39) В чем разница между необратимыми и обратимыми технологиями шифрования?

40) Какие компоненты должны использовать системы шифрования для организации защищенной передачи данных по незащищенным сетям?

41) В чем заключается алгоритм шифрования DES (Data Encryption Standard)?

42) Какие компоненты Access могут быть небезопасны?

43) Какие основные методы защиты базы данных предоставляет СУБД Microsoft Access?

44) Какие основные средства и инструменты, необходимые для построения защищенных систем СУБД Oracle?

45) Какие категории привилегий предусмотрены в СУБД Oracle?

6.6 Тематика и содержание курсовой работы

Курсовая работа не предусмотрена.

7 Учебно-методическое и информационное обеспечение дисциплины

7.1 Рекомендуемая литература

Основная литература

1. Окороков В.А. Безопасность операционных систем: учебное пособие для вузов / В.А. Окороков. — Санкт-Петербург: Лань, 2024. — 228 с. с ил. [Электронный ресурс]. – URL: https://lanbook.com/catalog/informatika/bezopasnost-operatsionnykh-sistem Режим доступа для авторизированных пользователей (Дата обращения 26.08.2024).

Дополнительная литература

1. Смирнов С.Н. Безопасность систем баз данных: учебное пособие для студентов высших учебных заведений, обучающихся по специальностям в области информационной безопасности / С. Н. Смирнов. — Москва: Гелиос АРВ, 2007. — 350, [1] с. : ил., табл. . + https://m.eruditor.one/file/1706071/?ysclid=m8eitc2r2r270425706 (Дата обращения 26.08.2024).

2. Безбогов А.А. Безопасность операционных систем: учебное пособие / А.А. Безбогов, А.В. Яковлев, Ю.Ф. Мартемьянов. – М.: "Издательство Машино строение-1", 2007. – 220 с. – [Электронный ресурс]: https://tstu.ru/book/elib/pdf/2007/k_Martemyanov.pdf. (Дата обращения 26.08.2024).

7.2 Базы данных, электронно-библиотечные системы, информационно-справочные и поисковые системы

1. Научная библиотека ДонГТУ : официальный сайт.— Алчевск. —URL: library.dstu.education. — Текст : электронный.

2. Научно-техническая библиотека БГТУ им. Шухова : официальный сайт. — Белгород. — URL: http://ntb.bstu.ru/jirbis2/. — Текст : электронный.

3. Консультант студента : электронно-библиотечная система.— Москва. — URL: http://www.studentlibrary.ru/cgi-bin/mb4x. — Текст : электронный.

4. Университетская библиотека онлайн: электронно-библиотечная система. – URL: http://biblioclub.ru/index.php?page=main_ub_red. – Текст : электронный.

5. IPR BOOKS : электронно-библиотечная система.—Красногорск. — URL: http://www.iprbookshop.ru/. — Текст : электронный.

6. Сайт кафедры ИСИБ http://scs.dstu.education.

8 Материально-техническое обеспечение дисциплины

Материально-техническая база обеспечивает проведение всех видов деятельности в процессе обучения, соответствует требованиям ФГОС ВО.

Материально-техническое обеспечение представлено в таблице 6.

Таблица 6 – Материально-техническое обеспечение

Наименование оборудованных учебных кабинетов	Адрес (местоположение) учебных кабинетов
Специальные помещения: *Мультимедийная аудитория. (60 посадочных мест)*, оборудованная специализированной (учебной) мебелью (парта трехместная – 18 шт., парта двухместная – 6 шт, стол– 1 шт., доска аудиторная– 1 шт.), учебное ПК (монитор + системный блок), мультимедийная стойка с оборудованием – 1 шт., широкоформатный экран. Аудитории для проведения лекций: *Компьютерные классы (22 посадочных места),* оборудованный учебной мебелью, компьютерами с неограниченным доступом к сети Интернет, включая доступ к ЭБС:	ауд. *207* корп. *4* ауд. *217* корп. 3 ауд. *211* корп. *4*

Лист согласования РПД

Разработал:

ст. преподаватель кафедры
интеллектуальных систем и
информационной безопасности
(должность)

(подпись) Р.Н. Погорелов
(Ф.И.О.)

И.о. заведующего кафедрой
интеллектуальных систем и
информационной безопасности
(наименование кафедры)

(подпись) Е.Е. Бизянов
(Ф.И.О.)

Протокол №__1__ заседания кафедры от __27.08. 2024г.

И.о. декана факультета
информационных технологий
и автоматизации производственных
процессов:
(наименование факультета)

(подпись) В.В. Дьячкова
(Ф.И.О.)

Согласовано

Председатель методической
комиссии по специальности 10.05.03
Информационная безопасность
автоматизированных систем

(подпись) Е.Е. Бизянов
(Ф.И.О.)

Начальник учебно-методического центра

(подпись) О.А. Коваленко
(Ф.И.О.)

Лист изменений и дополнений

<table>
<tr><td colspan="2">Номер изменения, дата внесения изменения, номер страницы для внесения изменений</td></tr>
<tr><td>ДО ВНЕСЕНИЯ ИЗМЕНЕНИЙ:</td><td>ПОСЛЕ ВНЕСЕНИЯ ИЗМЕНЕНИЙ:</td></tr>
<tr><td colspan="2">Основание:</td></tr>
<tr><td colspan="2">Подпись лица, ответственного за внесение изменений</td></tr>
</table>