Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ИРКУТСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Структурное подразделение «Институт информационных технологий и анализа данных»

УТВЕРЖДЕНА:
на заседании Совета института ИТиАД им. Е.И.Попова
Протокол №8 от 24 февраля 2025 г.

Рабочая программа дисциплины

«БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ»

Направление: 10.03.01 Информационная безопасность

Организация и технологии защиты информации (в сфере техники и технологии)

Квалификация: Бакалавр

Форма обучения: очная

Документ подписан простой электронной подписью Составитель программы: Мамедов Эльшан Фахраддинович Дата подписания: 16.06.2025	Документ подписан простой электронной подписью Утвердил: Говорков Алексей Сергеевич Дата подписания: 16.06.2025	Документ подписан простой электронной подписью Согласовал: Сибиряк Юрий Владимирович Дата подписания: 17.06.2025

Год набора – 2025

Иркутск, 2025 г.

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

1.1 Дисциплина «Безопасность операционных систем» обеспечивает формирование следующих компетенций с учётом индикаторов их достижения

Код, наименование компетенции	Код индикатора компетенции
ПКС-2 Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	ПКС-2.1
ПКС-3 Способность администрировать подсистемы информационной безопасности объекта защиты	ПКС-3.1

1.2 В результате освоения дисциплины у обучающихся должны быть сформированы

Код индикатора	Содержание индикатора	Результат обучения
ПКС-3.1	Способен поддерживать работоспособность операционных систем, управлять аппаратной частью компьютера и прикладными программами, а также осуществлять безопасность системной среды взаимодействия между компьютерными системами; владеет современными технологиями от атак злоумышленников	**Знать** назначение и виды архитектур информационных систем; особенности функционирования компьютеров в определенной архитектуре информационной системы; базисные принципы отражения архитектуры локальной сети на архитектуру информационных систем; функциональное разграничение программных компонентов информационной системы **Уметь** проводить анализ целесообразности использования той или иной архитектуры информационных систем; осуществлять базовую компоновку компьютерных ролей; анализировать пути оптимизации и модернизации архитектуры информационных системы; осуществлять покомпонентное деление архитектуры информационных систем в рамках реализуемого функционала **Владеть** навыками выбора архитектуры информационных систем в соответствии с предъявляемыми функциональными требованиями;

		навыками выбора программно-технических средств, применимых к определенной архитектуре информационных систем; средствами диагностики и поиска неисправностей; навыками оформления эксплуатационной документации в части архитектуры информационных систем
ПКС-2.1	Способен классифицировать безопасность ОС по различным аспектам их реализации (цели атак, по принципу воздействия на операционную систему, по типу используемой злоумышленником уязвимости защиты, по характеру воздействия на операционную систему); умеет в комплексе применять средства защиты от основных классов угроз	**Знать** Виды ОС. Процессы. Алгоритмы и механизмы синхронизации. Тупики. Управления памятью. Файлы. Реализация файловой системы. Система управления вводом-выводом. Угрозы безопасности ОС. Требования к защите ОС. Разграничение доступа в ОС. Идентификация и аутентификация пользователей ОС. Аудит в ОС. **Уметь** Управлять процессами в операционных системах. Разграничивать доступ к процессам. Работать с системами ввода-вывода. Строить модель угроз для ОС. Работать с правами и привилегиями для пользователей. Проводить аудит ОС. **Владеть** Средствами управления процессами. Методами и средствами работы с файловой системой. Навыками работы с конфигурационными файлами ОС. Средствами разграничения доступа. Средствами управления политиками безопасности ОС. Системами логирования.

2 Место дисциплины в структуре ООП

Изучение дисциплины «Безопасность операционных систем» базируется на результатах освоения следующих дисциплин/практик: «Информационные технологии», «Основы информационной безопасности», «Аудит информационной безопасности», «Теория информации», «Технологии и методы программирования», «Физические основы информационной безопасности», «Методы и средства криптографической защиты информации», «Нейронные сети», «Искусственный интеллект», «Реагирование на инциденты информационной безопасности», «Сети и системы передачи информации»

Дисциплина является предшествующей для дисциплин/практик: «Защита информации от утечки по техническим каналам», «Методы оценки безопасности

компьютерных систем», «Основы управления информационной безопасностью», «Безопасность сетей и баз данных»

3 Объем дисциплины

Объем дисциплины составляет – 3 ЗЕТ

Вид учебной работы	**Трудоемкость в академических часах** (Один академический час соответствует 45 минутам астрономического часа)	
	Всего	Семестр № 7
Общая трудоемкость дисциплины	108	108
Аудиторные занятия, в том числе:	64	64
лекции	32	32
лабораторные работы	0	0
практические/семинарские занятия	32	32
Самостоятельная работа (в т.ч. курсовое проектирование)	44	44
Трудоемкость промежуточной аттестации	0	0
Вид промежуточной аттестации (итогового контроля по дисциплине)	Зачет	Зачет

4 Структура и содержание дисциплины

4.1 Сводные данные по содержанию дисциплины

Семестр № 7

№ п/п	**Наименование раздела и темы дисциплины**	**Виды контактной работы**						СРС		**Форма текущего контроля**
		Лекции		ЛР		ПЗ(СЕМ)				
		№	Кол. Час.	№	Кол. Час.	№	Кол. Час.	№	Кол. Час.	
1	2	3	4	5	6	7	8	9	10	11
1	Введение	1	4			1	2	1, 2	44	Устный опрос
2	Структура ОС	2	6			2	6			Устный опрос
3	Файловые системы	3	4			3	6			Устный опрос
4	Процессы и потоки	4	6			4	6			Устный опрос
5	Администрирование ОС	5	6			5	6			Устный опрос
6	Безопасность ОС	6	6			6	6			Устный опрос
	Промежуточная аттестация									Зачет
	Всего		32				32		44	

4.2 **Краткое содержание разделов и тем занятий**

Семестр № 7

№	**Тема**	**Краткое содержание**

1	Введение	Общая характеристика ОС. История развития ОС. Назначение и функции ОС и ее подсистем. Системы разделения времени, пакетной обработки, реального времени. Управление ресурсами.
2	Структура ОС	Структура операционной системы. Типы ядра. Интерфейс ОС с пользователями. Управление памятью. Типы адресов. Структура виртуального адресного пространства процесса. Виртуальная память. Преобразование адресов. Методы распределения памяти. Защита памяти. Учет свободной и занятой памяти. Алгоритмы выбора вытесняемой страницы. Принципы работы кэшпамяти. Управление устройствами. Прерывания в ОС. Структура и функции подсистемы управления устройствами ввода-вывода. Системные сервисы ввода- вывода. Драйверы внешних устройств. Многоуровневые драйверы.
3	Файловые системы	Файловые системы. Физическая организация файловых систем. Логическая организация файловых систем. Физическая организация файла. Операции с файлами. Функциональные возможности файловых систем. Управление процессами. Типы программ, работа со службами. Организация динамических и статических вызовов.
4	Процессы и потоки	Процессы и потоки. Дескрипторы процесса и потока. Сохранение и восстановление процессов и потоков. Планирование потоков. Синхронизация процессов. Тупиковые ситуации. Наследование ресурсов. Межпроцессное взаимодействие.
5	Администрирование ОС	Администрирование ОС. Задачи и принципы сопровождения системного программного обеспечения. Настройка, измерение производительности и модификация ОС. Основные механизмы обеспечения безопасности ОС. Типовые угрозы безопасности ресурсов ОС.
6	Безопасность ОС	Требования к безопасности ОС. Основные группы механизмов защиты ресурсов ОС. Средства и методы аутентификации в ОС. Аутентификация на основе пароля. Аутентификация с использованием физического объекта. Биометрические методыаутентификации. Многофакторная аутентификация. Технология SSO. Разграничение доступа к ресурсам ОС. Классификация субъектов и объектов доступа. Права доступа. Методы разграничения доступа. Разграничение доступа кфайловым объектам. Наследование разрешений. Разграничение доступа к устройствам. Ограничения на запуск программного обеспечения. Контроль работы подсистемы

		защиты. Организация и использование средств аудита. Контроль и восстановление целостности подсистемы защиты и ее параметров. Управление безопасностью ОС.

4.3 Перечень лабораторных работ

Лабораторных работ не предусмотрено

4.4 Перечень практических занятий

Семестр № 7

№	Темы практических (семинарских) занятий	Кол-во академических часов
1	Введение	2
2	Структура ОС	6
3	Файловые системы	6
4	Процессы и потоки	6
5	Администрирование ОС	6
6	Безопасность ОС	6

4.5 Самостоятельная работа

Семестр № 7

№	Вид СРС	Кол-во академических часов
1	Подготовка к зачёту	24
2	Подготовка к практическим занятиям (лабораторным работам)	20

В ходе проведения занятий по дисциплине используются следующие интерактивные методы обучения: Дискуссия, Кейс-технология

5 Перечень учебно-методического обеспечения дисциплины

5.1 Методические указания для обучающихся по освоению дисциплины

5.1.1 Методические указания для обучающихся по практическим занятиям

https://el.istu.edu/course/index.php?categoryid=1107

5.1.2 Методические указания для обучающихся по самостоятельной работе:

https://el.istu.edu/course/index.php?categoryid=1107

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

6.1 Оценочные средства для проведения текущего контроля

6.1.1 семестр 7 | Устный опрос

Описание процедуры.

Проведение устного опроса в форме «вопрос-ответ»
Вопросы для контроля:
Разграничение доступа к ресурсам ОС. Методы разграничения доступа. Разграничение доступа к устройствам.

Критерии оценивания.

ответ раскрыт полностью – 5 баллов
ответ раскрыт частично – 2-4 баллов
имеет только общее представление о проблеме – 1 балл
не ответил – 0 баллов

6.2 Оценочные средства для проведения промежуточной аттестации

6.2.1 Критерии и средства (методы) оценивания индикаторов достижения компетенции в рамках промежуточной аттестации

Индикатор достижения компетенции	Критерии оценивания	Средства (методы) оценивания промежуточной аттестации
ПКС-3.1	Способен поддерживать работоспособность операционных систем, управлять аппаратной частью компьютера и прикладными программами, а также осуществлять безопасность системной среды взаимодействия между компьютерными системами; владеет современными технологиями от атак злоумышленников	Тестовые задания зачет
ПКС-2.1	Демонстрирует способность классифицировать безопасность ОС по различным аспектам их реализации (цели атак, по принципу воздействия на операционную систему, по типу используемой злоумышленником уязвимости защиты, по характеру воздействия на операционную систему)	Тестовые задания зачет

6.2.2 Типовые оценочные средства промежуточной аттестации

6.2.2.1 Семестр 7, Типовые оценочные средства для проведения зачета по дисциплине

6.2.2.1.1 Описание процедуры

Перечень теоретических вопросов, практических заданий и ситуаций, выносимых на экзамен, доводятся преподавателем до студентов в начале изучения программы.

Формулировки вопросов, заданий должны быть четкими, краткими, понятными, исключающими двойное толкование. Могут быть применены тестовые задания или задания комбинированного характера. Количество вариантов для устных заданий должно быть больше чем число студентов, сдающих экзамен не менее, чем на 3. Количество вариантов для письменных заданий должно быть не менее двух.

Примерный перечень вопросов к зачёту:

1. Общая характеристика ОС.
2. История развития ОС.
3. Назначение и функции ОС и ее подсистем.
4. Системы разделения времени, пакетной обработки, реального времени.
5. Управление ресурсами.
6. Структура операционной системы.
7. Типы ядра.
8. Интерфейс ОС с пользователями.
9. Управление памятью.
10. Типы адресов.
11. Структура виртуального адресного пространства процесса.
12. Виртуальная память.
13. Преобразование адресов.
14. Методы распределения памяти.
15. Защита памяти.
16. Учет свободной и занятой памяти.
17. Алгоритмы выбора вытесняемой страницы.
18. Принципы работы кэш-памяти.
19. Управление устройствами. Прерывания в ОС.
20. Структура и функции подсистемы управления устройствами ввода-вывода.
21. Системные сервисы ввода-вывода.
22. Драйверы внешних устройств.
23. Многоуровневые драйверы.
24. Файловые системы.
25. Физическая организация файловых систем.
26. Логическая организация файловых систем.
27. Физическая организация файла.
28. Операции с файлами.
29. Функциональные возможности файловых систем.
30. Управление процессами.
31. Типы программ, работа со службами.
32. Организация динамических и статических вызовов.
33. Процессы и потоки.
34. Дескрипторы процесса и потока.
35. Сохранение и восстановление процессов и потоков.
36. Планирование потоков.
37. Синхронизация процессов.
38. Тупиковые ситуации.
39. Наследование ресурсов.
40. Межпроцессное взаимодействие.
41. Администрирование ОС.
42. Задачи и принципы сопровождения системного программного обеспечения.
43. Настройка, измерение производительности и модификация ОС.
44. Основные механизмы обеспечения безопасности ОС.

45. Типовые угрозы безопасности ресурсов ОС.
46. Требования к безопасности ОС.
47. Основные группы механизмов защиты ресурсов ОС.
48. Средства и методы аутентификации в ОС.
49. Аутентификация на основе пароля.
50. Аутентификация с использованием физического объекта.
51. Биометрические методы аутентификации.
52. Многофакторная аутентификация.
53. Технология SSO.
54. Разграничение доступа к ресурсам ОС.
55. Классификация субъектов и объектов доступа.
56. Права доступа. Методы разграничения доступа.
57. Разграничение доступа к файловым объектам. Наследование разрешений.
58. Разграничение доступа к устройствам.
59. Ограничения на запуск программного обеспечения.
60. Контроль работы подсистемы защиты.
61. Организация и использование средств аудита.
62. Контроль и восстановление целостности подсистемы защиты и ее параметров.
63. Управление безопасностью ОС.

Пример задания:

1. Организация и использование средств аудита.
2. Контроль и восстановление целостности подсистемы защиты и ее параметров.
3. Управление безопасностью ОС.

6.2.2.1.2 Критерии оценивания

Зачтено	Не зачтено
Ответ правильный, логически выстроен, использована профессиональная терминология. Обучающийся правильно интерпретирует полученный результат.	Ответы неправильные или неполные.

7 Основная учебная литература

1. Рудаков А. В. Операционные системы и среды [Электронный ресурс] : учебник / А. В. Рудаков, 2022. - 304.

2. Батаев А. В. Операционные системы и среды : учебник для студентов среднего специального образования / А. В. Батаев, Н. Ю. Налютин, С. В. Синицин, 2021. - 288.

3. Бакшеева Е. Н. Операционные системы : электронный курс / Е. Н. Бакшеева, П. А. Петров, Е. Н. Лебедева, 2023

4. Каташевцев М. Д. Операционные системы : электронный курс / М. Д. Каташевцев, 2022

8 Дополнительная учебная литература и справочная

1. Таненбаум Э. Современные операционные системы / Э. Таненбаум, Х. Бос, 2022. - 1120.

2. Староверова Н. А. Операционные системы : учебник / Н. А. Староверова, 2023. - 308.

9 Ресурсы сети Интернет

1. http://library.istu.edu/
2. https://e.lanbook.com/

10 Профессиональные базы данных

1. http://new.fips.ru/
2. http://www1.fips.ru/

11 Перечень информационных технологий, лицензионных и свободно распространяемых специализированных программных средств, информационных справочных систем

1. Microsoft DreamSpark Premium Electronic Software Delivery_2018

2. Microsoft Office 2007 Standard - 2003 Suites и 2007 Suites - поставка 2010

12 Материально-техническое обеспечение дисциплины

1. Проектор мультимедиа BenQ MW621ST(с экраном 3*3 м)

2. Экран ScreenMedia GoldView 274*206 настенный