МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Филиал КузГТУ в г. Новокузнецке

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 71B13ADF852F0D849D78875814FBEF47
Владелец: Баранов Юрий Александрович
Действителен: с 15.10.2025 до 08.01.2027

УТВЕРЖДЕНО

Заместитель директора,
совмещающий обязанности директора
филиала КузГТУ в г. Новокузнецке

_____Баранов Ю.А.

«29» мая 2026г.

Рабочая программа дисциплины

Безопасность операционных систем

Направление подготовки 10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль) Анализ безопасности информационных систем

Присваиваемая квалификация «Специалист по защите информации»

Формы обучения: очная

Год набора 2026

Новокузнецк 2026 г.

Рабочая программа обсуждена на заседании учебно-методического совета филиала КузГТУ в г. Новокузнецке

Протокол № 6 от 29.05.2026

Зав. Кафедрой ИТиЭД _____ В. В. Шарлай
подпись

СОГЛАСОВАНО:

Заместитель директора по УР _____ Т. А. Евсина
подпись

1 Перечень планируемых результатов обучения по дисциплине "Безопасность операционных систем", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:

общепрофессиональных компетенций:

ОПК-12 - Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем;

Результаты обучения по дисциплине определяются индикаторами достижения компетенций

Индикатор(ы) достижения:

Применяет знания в области безопасности операционных систем

Результаты обучения по дисциплине:

Знать принципы построения и функционирования, примеры реализаций современных операционных систем; функции операционных систем, основные концепции управления процессорами, памятью, вспомогательной памятью, устройствами; критерии оценки эффективности и надежности средств защиты операционных систем; принципы организации и структуру подсистем защиты операционных систем семейств UNIX и Windows.

Уметь использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; оценивать эффективность и надежность защиты операционных систем; планировать политику безопасности операционных систем.

Владеть профессиональной терминологией в области информационной безопасности; навыками работы с операционными системами семейств UNIX и Windows, восстановление операционных систем после сбоев; навыками установки и настройки операционных систем семейств UNIX и Windows с учетом требований по обеспечению информационной безопасности; навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности.

2 Место дисциплины "Безопасность операционных систем" в структуре ОПОП специалитета

Для освоения дисциплины необходимы знания умения, навыки и (или) опыт профессиональной деятельности, полученные в рамках изучения следующих дисциплин: Основы информационной безопасности, Основы информатики, организации ЭВМ, вычислительных и информационных систем, Информационные угрозы, Классификация защищаемой информации и информационных систем.

Дисциплина входит в Блок 1 «Дисциплины (модули)» ОПОП. Цель дисциплины - получение обучающимися знаний, умений, навыков и (или) опыта профессиональной деятельности, необходимых для формирования компетенций, указанных в пункте 1.

3 Объем дисциплины "Безопасность операционных систем" в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины "Безопасность операционных систем" составляет 9 зачетных единиц, 324 часа.

Форма обучения	**Количество часов**		
	ОФ	**ЗФ**	**ОЗФ**
Курс 2/Семестр 4			
Всего часов	144		
Контактная работа обучающихся с преподавателем (по видам учебных занятий):			
Аудиторная работа			
Лекции			
Лабораторные занятия			

Форма обучения	Количество часов		
	ОФ	ЗФ	ОЗФ
Практические занятия	32		
Внеаудиторная работа			
Индивидуальная работа с преподавателем:			
Консультация и иные виды учебной деятельности			
Самостоятельная работа под руководством преподавателя	16		
Самостоятельная работа	60		
Форма промежуточной аттестации	экзамен /36		
Курс 3/Семестр 5			
Всего часов	180		
Контактная работа обучающихся с преподавателем (по видам учебных занятий):			
Аудиторная работа			
Лекции			
Лабораторные занятия			
Практические занятия	32		
Внеаудиторная работа			
Индивидуальная работа с преподавателем:			
Консультация и иные виды учебной деятельности			
Самостоятельная работа под руководством преподавателя	48		
Самостоятельная работа	100		
Форма промежуточной аттестации	зачет		

4 Содержание дисциплины "Безопасность операционных систем", структурированное по разделам (темам)

4.1. Лекционные занятия

Раздел дисциплины, темы лекций и их содержание	Трудоемкость в часах
	ОФ
5 семестр	
1. Архитектура современных ОС.	
1.1 Введение в операционные системы. Процессы. Алгоритмы и механизмы синхронизации. Тупики	4
1.2 Управление памятью. Файловая система. Система ввода-вывода.	6
1.3. Механизмы синхронизации процессов и потоков.	6
Итого	**16**
6 семестр	
2. Защита информации в современных ОС.	
2.1 Угрозы безопасности ОС. Требования к защите ОС. Разграничение доступа в ОС.	8
2.2. Идентификация и аутентификация пользователей ОС. Аудит в ОС.	8
Итого	**16**

4.2. Лабораторные занятия

Наименование работы	**Трудоемкость в часах**
	ОФ
5 семестр	
1. Алгоритмы и механизмы синхронизации.	4
2. Управление памятью.	6
3. Файловая система.	6
4. Система ввода-вывода.	4
5. Консольные приложения.	4
6. Методы управления процессами.	4
7. Методы управления потоками.	4
Итого	**32**
6 семестр	
1. Угрозы безопасности ОС.	4
2. Требования к защите ОС.	4
3. Разграничение доступа в ОС.	6
4. Идентификация и аутентификация пользователей ОС.	6
5. Аудит в ОС.	4
6. Механизмы межпроцессорного взаймодействия(общий сегмент памяти)	4
7. Механизмы межпроцессорного взаймодействия(семафоры)	4
Итого	**32**

4.3 Самостоятельная работа обучающегося и перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Вид СРС	**Трудоемкость в часах**
	ОФ
5 семестр	
Ознакомление с содержанием основной и дополнительной литературы, методических материалов, конспектов лекций для подготовки к занятиям	18
Оформление отчетов по практическим и(или) лабораторным работам	20
Подготовка к промежуточной аттестации	6

Итого	**44**
Экзамен	36
Самостоятельная работа под руководством преподавателя	16
6 семестр	
Ознакомление с содержанием основной и дополнительной литературы, методических материалов, конспектов лекций для подготовки к занятиям	30
Оформление отчетов по практическим и(или) лабораторным работам	28
Подготовка к промежуточной аттестации	6
Итого	**64**
Самостоятельная работа под руководством преподавателя	32

5 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине "Безопасность операционных систем"

5.1 Паспорт фонда оценочных средств

Планируемые результаты обучения по дисциплине (модулю)
Дисциплина направлена на формирование следующих компетенций выпускника:

Форма(ы) текущего контроля	Компетенции, формируемые в результате освоения дисциплины (модуля)	Индикатор(ы) достижения компетенции	Результаты обучения по дисциплине (модулю)	Уровень

Опрос по контрольным вопросам или тестирование, подготовка отчетов по практическим и(или) лабораторным работам	ОПК-12 - Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем	Применяет знания в области безопасности операционных систем	**Знать** принципы построения и функционирования, примеры реализаций современных операционных систем; функции операционных систем, основные концепции управления процессорами, памятью, вспомогательной памятью, устройствами; критерии оценки эффективности и надежности средств защиты операционных систем; принципы организации и структуру подсистем защиты операционных систем семейств UNIX и Windows. **Уметь** использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; оценивать эффективность и надежность защиты операционных систем; планировать политику безопасности операционных систем. **Владеть** профессиональной терминологией в области информационной безопасности; навыками работы с операционными системами семейств UNIX и Windows, восстановление операционных систем после сбоев; навыками установки и настройки операционных систем семейств UNIX и Windows с учетом требований по обеспечению информационной безопасности; навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности.	Высокий или средний
Высокий уровень достижения компетенции - компетенция сформирована частично, рекомендованные оценки: отлично, хорошо, зачтено. **Средний уровень достижения компетенции** - компетенция сформирована частично, рекомендованные оценки: хорошо, удовлетворительно, зачтено. **Низкий уровень достижения компетенции** - компетенция не сформирована частично, оценивается неудовлетворительно или не зачтено.				

5.2. Типовые контрольные задания или иные материалы

Текущий контроль успеваемости и аттестационные испытания обучающихся могут быть

организованы с использованием ресурсов ЭИОС КузГТУ. Полный перечень оценочных материалов расположен в ЭИОС КузГТУ.: https://el.kuzstu.ru/login/index.php.

Текущий контроль успеваемости и аттестационные испытания могут проводиться в письменной и (или) устной, и (или) электронной форме.

5.2.1.Оценочные средства при текущем контроле

Текущий контроль по дисциплине будет заключаться в опросе обучающихся по контрольным вопросам или тестирование по разделу дисциплины, оформлении оформлении отчетов по практическим и(или) лабораторным работам.

Опросе обучающихся по контрольным вопросам или тестирование по разделу дисциплины

Обучающийся отвечает на 2 вопроса, либо отвечает на 10 тестовых заданий.

Критерии оценивания при ответе на вопросы:

- 100 баллов – при правильном и полном ответе на два вопроса;
- 85…99 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 75…84 баллов – при правильном и неполном ответе на два вопроса;
- 65…74 баллов – правильном и полном ответе только на один из вопросов
- 25…64 – при правильном и неполном ответе только на один из вопросов;
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–64	65–100
Шкала оценивания	Не зачтено	Зачтено

Критерии оценивания при тестировании:

- 100 баллов – при правильном и полном ответе на 10 вопросов;
- 85…99 баллов – при правильном ответе на 8-9 вопросов;
- 75…84 баллов – при правильном ответе на 7 вопросов;
- 65…74 баллов – правильном ответе на 5-6 вопросов
- 25…64 – при правильном ответе только на 4 вопроса;
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–64	65–100
Шкала оценивания	Не зачтено	Зачтено

Примерный перечень контрольных вопросов:

1. Архитектура современных ОС

1.1 Введение в операционные системы. Процессы. Алгоритмы и механизмы синхронизации. Тупики

1. Основные функции, выполняемые операционными системами
2. Понятие процесса. Состояния процесса
3. Какой процесс обязательно должен выполняться в системе памяти с перемещаемыми разделами
4. Требования к алгоритмам, организующим взаимодействия процессов, имеющих критические участки
5. Суть тупиковой ситуации. Модель Холта

1.2 Управление памятью. Файловая система. Система ввода-вывода.

1. Страничная организация памяти
2. Сегментная организация памяти
3. Назначение и основные функции файловой системы
4. Подсистема ввода-вывода в ядре ОС
5. Производительность систем ввода-вывода

1.3. Механизмы синхронизации процессов и потоков.

1. Аппаратная поддержка синхронизации процессов
2. Классические проблемы синхронизации процессов
3. Цели и средства синхронизации

4. Условия, при которых необходима синхронизация потоков и процессов
5. Синхронизация на основе общих семафоров

2. Защита информации в современных ОС.

2.1 Угрозы безопасности ОС. Требования к защите ОС. Разграничение доступа в ОС.

1. Классификация угроз безопасности ОС
2. Понятие защищенной операционной системы
3. Основные функции подсистемы защиты операционной системы
4. Понятия объекта, субъекта, метода доступа к объекту.
5. Основные модели разграничения доступа

2.2. Идентификация и аутентификация пользователей ОС. Аудит в ОС.

1. Понятия идентификации, аутентификации и авторизации пользователей
2. Наиболее распространенными методами идентификации и аутентификации
3. Понятие аудита в ОС и его цели
4. Требования к аудиту в операционных системах
5. Классификация процессов аутентификации по уровню обеспечиваемой безопасности

Примерный перечень тестовых заданий:

1. Архитектура современных ОС

1.1 Введение в операционные системы. Процессы. Алгоритмы и механизмы синхронизации. Тупики

1. Операционная система относится к …

Прикладному программному обеспечению
Системному программному обеспечению
Инструментальному программному обеспечению
К базовой системе ввода-вывода

2. Что такое процесс?

экземпляр выполняемой программы
ход выполнения программы
попеременное выполнение нескольких программ на одном процессоре

3. К условиям возникновения тупиков относятся: выбрать все верные

Условие взаимоисключения
Условие ожидания ресурсов
Условие синхронизации
Условие кругового ожидания

1.2 Управление памятью. Файловая система. Система ввода-вывода.

1. Какие виды организации памяти используются в концепции виртуальной памяти: выбрать все верные

страничная организация
сегментная организация
сегментно-страничная организация
с динамическими разделами
с фиксированными разделами

2. Одноуровневая файловая система:

каталог диска представляет собой иерархическую последовательность имён файлов
представляет собой систему вложенных папок
когда каталог диска представляет собой линейную последовательность имён файлов и соответствующих начальных секторов
каталог диска представляет собой геометрическую последовательность имён файлов

3. Какая существует классификация операций ввода-вывода? Выбрать все верные

по способу ввода-вывода на устройства
по обработке данных перед выводом
по типам устройств, на которые осуществляется вывод

1.3. Механизмы синхронизации процессов и потоков.

1. Для синхронизации потоков прикладных программ программист может использовать:

собственные средства и приемы синхронизации
средства операционной системы
оба ответа верны

2. Критическая секция это:

часть программы, результат выполнения которой может непредсказуемо меняться, если переменные, относящиеся к этой части программы, изменяются другими потоками в то время, когда выполнение этой части еще не завершено
Область памяти или буфер, который может опустошаться, и в следствии чего в программе возникает ошибка из-за отсутствия данных.
Часть программы, в которой процессам не хватает ресурсов

3. Какие объекты синхронизации процессов и потоков используются чаще всего в ОС: выбрать все верные:

События
Мъютексы
Семафоры
Системные вызовы
Блокирующие переменные

2. Защита информации в современных ОС.

2.1 Угрозы безопасности ОС. Требования к защите ОС. Разграничение доступа в ОС.

1. Под уязвимостью защиты ОС понимается…

свойство ОС (недостаток), которое может быть использовано злоумышленником для проникновения из внешних систем в ОС
свойство ОС (недостаток), которое может быть использовано злоумышленником для осуществления неправильной настройки систем безопасности
свойство ОС (недостаток), которое может быть использовано злоумышленником для осуществления несанкционированного доступа к информации

2. От каких действий должна защищать подсистема безопасности ОС?

от несанкционированного доступа
от случайного ввода неверной информации
от злонамеренной модификации или разрушения
от неверного ввода информации пользователем в различных приложениях
от фишинга
от спуффинга

3. Основные методы разграничения доступа в ОС: выбрать все верные

дискреционный
мандатный
глобальный
интегральный
локальный

2.2. Идентификация и аутентификация пользователей ОС. Аудит в ОС.

1. Как называется процесс распознавание участника информационного взаимодействия перед тем, как к нему будут применены какие-либо аспекты ИБ:

идентификация
аутентификация

авторизация

2. Сервер аутентификации Kerberos:

не защищает от атак на доступность
частично защищает от атак на доступность
полностью защищает от атак на доступность

3. Укажите задачи, решаемые за счёт осуществления аудита: выбрать все верные

Обеспечение подотчётности пользователей и администраторов
Обнаружение попыток нарушения информационной безопасности
Обеспечение возможности восстановления хода событий при расследовании инцидентов, связанных с информационной безопасностью
Выявление неверно настроенных правил и политик информационной безопасности

Отчеты по лабораторным и (или) практическим работам (далее вместе - работы):

По каждой работе обучающиеся самостоятельно оформляют отчеты в электронном формате (согласно перечню лабораторных и(или) практических работ п.4 рабочей программы).

Содержание отчета:

1.Тема работы.

2. Задачи работы.

3. Краткое описание хода выполнения работы.

4. Ответы на задания или полученные результаты по окончании выполнения работы (в зависимости от задач, поставленных в п. 2).

5. Выводы

Критерии оценивания:

- 75 – 100 баллов – при раскрытии всех разделов в полном объеме
- 0 – 74 баллов – при раскрытии не всех разделов, либо при оформлении разделов в неполном объеме.

Количество баллов	0–74	75–100
Шкала оценивания	Не зачтено	Зачтено

5.2.2 Оценочные средства при промежуточной аттестации

Формами промежуточной аттестации являютя зачет, экзамен, в процессе которых определяются сформированность обозначенных в рабочей программе компетенций.

Инструментом измерения сформированности компетенций являются:

ответы на вопросы во время опроса по разделам дисциплины или пройденное тестирование.
зачтенные отчеты обучающихся по лабораторным и(или) практическим работам;

На зачете/экзамене обучающийся отвечает на 2 вопроса, либо отвечает на 20 тестовых заданий

Критерии оценивания при ответе на вопросы:

- 100 баллов – при правильном и полном ответе на два вопроса;
- 85…99 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 75…84 баллов – при правильном и неполном ответе на два вопроса;
- 65…74 баллов – правильном и полном ответе только на один из вопросов
- 25…64 – при правильном и неполном ответе только на один из вопросов;
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–24	25-64	65-74	85-99	100
Шкала оценивания	Неуд		Хорошо	Отлично	
	не зачтено		зачтено		

Критерии оценивания при тестировании:

- 95-100 баллов – при правильном и полном ответе на 19-20 вопросов;
- 85…94 баллов – при правильном ответе на 16-18 вопросов;
- 75…84 баллов – при правильном ответе на 13-15 вопросов;
- 65…74 баллов – правильном ответе на 10-12 вопросов
- 25…64 – при правильном ответе только на 1-9 вопрос(ов);
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–24	25-64	65-74	85-94	95-100
Шкала оценивания	Неуд		Хорошо	Хорошо	Отлично
	не зачтено		зачтено		

5 семестр:

Примерный перечень вопросов на экзамен:

1. Какими основными дефектами обладают операционные системы с точки зрения обеспечения безопасности данных?
2. Какие существуют способы реализации защиты операционных систем?
3. Для чего необходимы средства профилактического контроля безопасности операционные системы?
4. Что представляет собой и для чего применяется матрица доступа?
5. Что представляют собой и для чего применяются списки доступа?
6. В чем заключаются улучшения безопасности в ОС Windows 10?
7. Какие требования предъявляются к параметрам пароля для ОС Linux?
8. Как в ОС Linux отключить доступ к консольным программам?
9. Какие дополнительные функции обеспечения информационной безопасности появились в Internet Explorer 11?
10. В чем состоят противоречия между реализованными в ОС механизмами защиты и принятыми формализованными требованиями?
11. В чем, с точки зрения обеспечения информационной безопасности, состоит отличие между централизованной и распределенной схемой администрирования?
12. Как реализуется структура прав доступа к файлу в системе Unix?
13. Какие уровни доступа реализованы на уровне файловой системы в UNIX?
14. Какие основные защитные механизмы реализованы в системе Unix?
15. Каковы основные недостатки защитных механизмов ОС семейства Unix?
16. Какие основные защитные механизмы реализованы в ОС семейства Windows NT?
17. Какие основные функции управления учетными записями пользователей реализованы в ОС семейства Windows NT, влияющие на информационную безопасность?
18. Для чего предназначена служба Active Directory и какие она предоставляет возможности администрирования с точки зрения информационной безопасности?
19. Каким образом система Kerberos реализует попарную проверку подлинности субъектов.
20. Какие выделяют группы методов, позволяющие несанкционированно вмешаться в работу операционной системы?
21. Какие основные недостатки механизма защиты ОС используют средства несанкционированного доступа?
22. Безопасность файловой системы NTFS

Примерный перечень тестовых заданий на экзамен:

1. Операционная система относится к …

Прикладному программному обеспечению
Системному программному обеспечению
Инструментальному программному обеспечению
К базовой системе ввода-вывода

2. Что такое процесс?

экземпляр выполняемой программы
ход выполнения программы
попеременное выполнение нескольких программ на одном процессоре

3. К условиям возникновения тупиков относятся: выбрать все верные

Условие взаимоисключения
Условие ожидания ресурсов
Условие синхронизации
Условие кругового ожидания

4. Какие виды организации памяти используются в концепции виртуальной памяти: выбрать все верные

страничная организация
сегментная организация
сегментно-страничная организация
с динамическими разделами
с фиксированными разделами

5. Одноуровневая файловая система:

каталог диска представляет собой иерархическую последовательность имён файлов
представляет собой систему вложенных папок
когда каталог диска представляет собой линейную последовательность имён файлов и соответствующих начальных секторов
каталог диска представляет собой геометрическую последовательность имён файлов

6. Какая существует классификация операций ввода-вывода? Выбрать все верные

по способу ввода-вывода на устройства
по обработке данных перед выводом
по типам устройств, на которые осуществляется вывод

7. Для синхронизации потоков прикладных программ программист может использовать:

собственные средства и приемы синхронизации
средства операционной системы
оба ответа верны

8. Критическая секция это:

часть программы, результат выполнения которой может непредсказуемо меняться, если переменные, относящиеся к этой части программы, изменяются другими потоками в то время, когда выполнение этой части еще не завершено
Область памяти или буфер, который может опустошаться, и в следствии чего в программе возникает ошибка из-за отсутствия данных.
Часть программы, в которой процессам не хватает ресурсов

9. Какие объекты синхронизации процессов и потоков используются чаще всего в ОС: выбрать все верные:

События
Мъютексы
Семафоры
Системные вызовы
Блокирующие переменные

6 семестр:

Примерный перечень вопросов на зачет:

1. Контроль доступа к файлам в современных ОС
2. Основные понятия безопасности ОС
3. Системный подход к обеспечению безопасности в ОС
4. Аутентификация в ОС
5. Цифровые сертификаты и цифровые подписи как элемент информационной безопасности при работе в ОС
6. Авторизация доступа в ОС
7. Аудит безопасности в ОС
8. Протокол безопасных соединений SSH

Примерный перечень тестовых заданий на зачет:

1. Под уязвимостью защиты ОС понимается…

свойство ОС (недостаток), которое может быть использовано злоумышленником для проникновения из внешних систем в ОС
свойство ОС (недостаток), которое может быть использовано злоумышленником для осуществления неправильной настройки систем безопасности
свойство ОС (недостаток), которое может быть использовано злоумышленником для осуществления несанкционированного доступа к информации

2. От каких действий должна защищать подсистема безопасности ОС?

от несанкционированного доступа
от случайного ввода неверной информации
от злонамеренной модификации или разрушения
от неверного ввода информации пользователем в различных приложениях
от фишинга
от спуффинга

3. Основные методы разграничения доступа в ОС: выбрать все верные

дискреционный
мандатный
глобальный
интегральный
локальный

4. Как называется процесс распознавание участника информационного взаимодействия перед тем, как к нему будут применены какие-либо аспекты ИБ:

идентификация
аутентификация
авторизация

5. Сервер аутентификации Kerberos:

не защищает от атак на доступность
частично защищает от атак на доступность
полностью защищает от атак на доступность

6. Укажите задачи, решаемые за счёт осуществления аудита: выбрать все верные

Обеспечение подотчётности пользователей и администраторов
Обнаружение попыток нарушения информационной безопасности
Обеспечение возможности восстановления хода событий при расследовании инцидентов, связанных с информационной безопасностью
Выявление неверно настроенных правил и политик информационной безопасности

5.2.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций

1. Текущий контроль успеваемости обучающихся, осуществляется в следующем порядке: в конце завершения освоения соответствующей темы обучающиеся, по распоряжению педагогического работника, убирают все личные вещи, электронные средства связи и печатные источники информации.

Для подготовки ответов на вопросы обучающиеся используют чистый лист бумаги любого размера и ручку. На листе бумаги обучающиеся указывают свои фамилию, имя, отчество (при наличии), номер учебной группы и дату проведения текущего контроля успеваемости.

Научно-педагогический работник устно задает два вопроса, которые обучающийся может записать на подготовленный для ответа лист бумаги.

В течение установленного научно-педагогическим работником времени обучающиеся письменно формулируют ответы на заданные вопросы. По истечении указанного времени листы бумаги с подготовленными ответами обучающиеся передают научно-педагогическому работнику для

последующего оценивания результатов текущего контроля успеваемости.

При подготовке ответов на вопросы обучающимся запрещается использование любых электронных и печатных источников информации. В случае обнаружения научно-педагогическим работником факта использования обучающимся при подготовке ответов на вопросы указанные источники информации – оценка результатов текущего контроля соответствует 0 баллов и назначается дата повторного прохождения текущего контроля успеваемости.

Текущий контроль успеваемости обучающихся по результатам выполнения лабораторных и (или) практических работ осуществляется в форме отчета, который предоставляется научно-педагогическому работнику на бумажном и (или) электронном носителе. Научно-педагогический работник, после проведения оценочных процедур, имеет право вернуть обучающемуся отчет для последующей корректировки с указанием перечня несоответствий. Обучающийся обязан устранить все указанные несоответствия и направить отчет научно-педагогическому работнику в срок, не превышающий трех учебных дней, следующих за днем проведения текущего контроля успеваемости.

Результаты текущего контроля доводятся до сведения обучающихся в течение трех учебных дней, следующих за днем проведения текущего контроля успеваемости.

Обучающиеся, которые не прошли текущий контроль успеваемости в установленные сроки, обязаны пройти его в срок до начала процедуры промежуточной аттестации по дисциплине в соответствии с расписанием промежуточной аттестации.

Результаты прохождения процедур текущего контроля успеваемости обучающихся учитываются при оценивании результатов промежуточной аттестации обучающихся.

1. Промежуточная аттестация обучающихся проводится после завершения обучения по дисциплине в семестре в соответствии с календарным учебным графиком и расписанием промежуточной аттестации.

Для успешного прохождения процедуры промежуточной аттестации по дисциплине обучающиеся должны:

1. получить положительные результаты по всем предусмотренным рабочей программой формам текущего контроля успеваемости;
2. получить положительные результаты аттестационного испытания.

Для успешного прохождения аттестационного испытания обучающийся в течение времени, установленного научно-педагогическим работником, осуществляет подготовку ответов на два вопроса, выбранных в случайном порядке.

Для подготовки ответов используется чистый лист бумаги и ручка.

На листе бумаги обучающиеся указывают свои фамилию, имя, отчество (при наличии), номер учебной группы и дату проведения аттестационного испытания.

При подготовке ответов на вопросы обучающимся запрещается использование любых электронных и печатных источников информации.

По истечении указанного времени, листы с подготовленными ответам на вопросы обучающиеся передают научно-педагогическому работнику для последующего оценивания результатов промежуточной аттестации.

В случае обнаружения научно-педагогическим работником факта использования обучающимся при подготовке ответов на вопросы указанные источники информации – оценка результатов промежуточной аттестации соответствует 0 баллов и назначается дата повторного прохождения аттестационного испытания.

Результаты промежуточной аттестации обучающихся размещаются в ЭИОС КузГТУ.

Текущий контроль успеваемости и промежуточная аттестация обучающихся могут быть организованы с использованием ЭИОС КузГТУ, порядок и формы проведения текущего контроля успеваемости и промежуточной аттестации обучающихся при этом не меняется.

6 Учебно-методическое обеспечение

6.1 Основная литература

1. Ложников, П. С. Средства безопасности операционной системы ROSA Linux : учебное пособие : [16+] / П. С. Ложников, А. О. Провоторский. – Омск : Омский государственный технический университет (ОмГТУ), 2017. – 94 с. : табл., ил. – Режим доступа: по подписке. – URL:

https://biblioclub.ru/index.php?page=book&id=493349 (дата обращения: 17.04.2026). – Библиогр. в кн. – ISBN 978-5-8149-2502-2. – Текст : электронный.

2. Власенко, А. Ю. Операционные системы : учебное пособие : [16+] / А. Ю. Власенко, С. Н. Карабцев, Т. С. Рейн. – Кемерово : Кемеровский государственный университет, 2019. – 161 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=574269 (дата обращения: 09.04.2026). – Библиогр. в кн. – ISBN 978-5-8353-2424-8. – Текст : электронный.

3. Куль, Т. П. Операционные системы : учебное пособие : [16+] / Т. П. Куль. – Минск : РИПО, 2019. – 312 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=599951 (дата обращения: 10.04.2026). – Библиогр. в кн. – ISBN 978-985-503-940-3. – Текст : электронный.

4. Жидков, О. М. Сетевые операционные системы / О. М. Жидков. – Москва : Лаборатория книги, 2011. – 114 с. : табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=142238 (дата обращения: 14.04.2026). – ISBN 978-5-504-00184-5. – Текст : электронный.

5. Киренберг, А. Г. Информационная безопасность современных операционных систем : учебное пособие по дисциплине "Безопасность операционных систем" для студентов специальности 10.05.03 "Информационная безопасность автоматизированных систем" / А. Г. Киренберг ; Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, 2022. – 1 файл (1,48 Мб). – URL: http://library.kuzstu.ru/meto.php?n=91889&type=utchposob:common (дата обращения: 23.03.2026). – Текст : электронный.

6.2 Дополнительная литература

1. Введение в операционные системы и основы программирования : учебно-методическое пособие / Г. П. Аверьянов, В. А. Будкин, В. В. Дмитриева, И. А. Кунов. — Москва : НИЯУ МИФИ, 2015. — 260 с. — ISBN 978-5-7262-1994-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/119473 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

2. Сычев, О. А. Лабораторный практикум по дисциплине «Операционные системы». Клиент-серверные приложения : учебно-методическое пособие / О. А. Сычев, Е. Д. Беришева. — Волгоград : ВолгГТУ, 2019. — 64 с. — ISBN 978-5-9948-3440-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/157227 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

3. Сычев, О. А. Лабораторный практикум по дисциплине «Операционные системы». Управление процессами : учебно-методическое пособие / О. А. Сычев, Е. Д. Беришева. — Волгоград : ВолгГТУ, 2018. — 64 с. — ISBN 978-5-9948-3027-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/157226 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

4. Кобылянский, В. Г. Операционные системы, среды и оболочки : учебное пособие / В. Г. Кобылянский. — Санкт-Петербург : Лань, 2020. — 120 с. — ISBN 978-5-8114-4192-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/126937 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

5. Власенко, А. Ю. Операционные системы : учебное пособие / А. Ю. Власенко, С. Н. Карабцев, Т. С. Рейн. — Кемерово : КемГУ, 2019. — 161 с. — ISBN 978-5-8353-2424-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/121996 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

6.3 Методическая литература

1. Безопасность операционных систем : методические материалы для обучающихся специальности 10.05.03 "Информационная безопасность автоматизированных систем" очной формы обучения / ФГБОУ ВО "Кузбас. гос. техн. ун-т им. Т. Ф. Горбачева", Каф. информ. безопасности ; сост.: Е. В. Прокопенко, И. В. Чичерин. – Кемерово : КузГТУ, 2018. – 46 с. – URL: http://library.kuzstu.ru/meto.php?n=4633 (дата обращения: 23.03.2026). – Текст : электронный.

6.4 Профессиональные базы данных и информационные справочные системы

1. База данных Springer Materials http://materials.springer.com/

2. База данных zbMath https://zbmath.org/

3. Цифровая библиотека IPRsmart https://ipr-smart.ru/

4. Электронная библиотечная система «Университетская библиотека онлайн» http://biblioclub.ru/

5. Электронная библиотека КузГТУ https://library.kuzstu.ru/index.php/punkt-2/podrazdel-21

6. Электронная библиотека Новосибирского государственного технического университета https://clck.ru/UoXpv

7. Образовательная платформа «Юрайт» https://urait.ru/

8. Национальная электронная библиотека https://rusneb.ru/

9. Базы данных Springer Journals, Springer eBooks https://link.springer.com/

6.5 Периодические издания

1. Автоматика и телемеханика : журнал https://eivis.ru/browse/publication/79296

2. Безопасность информационных технологий: научный журнал https://eivis.ru/browse/publication/379646

3. Вестник Кузбасского государственного технического университета : научно-технический журнал https://vestnik.kuzstu.ru/

4. Информационные системы и технологии : научно-технический журнал https://eivis.ru/browse/publication/542286

5. Информационные технологии и вычислительные системы : журнал https://elibrary.ru/contents.asp?titleid=8746

6. Информация и безопасность : научный журнал

7. Программные продукты и системы : международный научно-практический журнал

7 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

ЭИОС КузГТУ:

a) Электронная библиотека КузГТУ. – Текст: электронный // Научно-техническая библиотека Кузбасского государственного технического университета им. Т. Ф. Горбачева : сайт. – Кемерово, 2001 – . – URL: https://elib.kuzstu.ru/. – Текст: электронный.

b) Портал.КузГТУ : Автоматизированная Информационная Система (АИС) : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://portal.kuzstu.ru/. – Режим доступа: для авториз. пользователей. – Текст: электронный.

c) Электронное обучение : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://el.kuzstu.ru/. – Режим доступа: для авториз. пользователей КузГТУ. – Текст: электронный.

8 Методические указания для обучающихся по освоению дисциплины "Безопасность операционных систем"

Самостоятельная работа обучающегося является частью его учебной деятельности, объемы самостоятельной работы по каждой дисциплине (модулю) практике, государственной итоговой аттестации, устанавливаются в учебном плане.

Самостоятельная работа по дисциплине (модулю), практике организуется следующим образом:

1. До начала освоения дисциплины обучающемуся необходимо ознакомиться с содержанием рабочей программы дисциплины (модуля), программы практики в следующем порядке:

1.1 содержание знаний, умений, навыков и (или) опыта профессиональной деятельности, которые будут сформированы в процессе освоения дисциплины (модуля), практики;

1.2 содержание конспектов лекций, размещенных в электронной информационной среде КузГТУ в порядке освоения дисциплины, указанном в рабочей программе дисциплины (модуля), практики;

1.3 содержание основной и дополнительной литературы.

2. В период освоения дисциплины обучающийся осуществляет самостоятельную работу в следующем порядке:

2.1 выполнение практических и (или) лабораторных работы и (или) отчетов в порядке, установленном в рабочей программе дисциплины (модуля), практики;

2.2 подготовка к опросам и (или) тестированию в соответствии с порядком, установленном в рабочей программе дисциплины (модуля), практики;

2.3 подготовка к промежуточной аттестации в соответствии с порядком, установленном в рабочей программе дисциплины (модуля), практики.

В случае затруднений, возникших при выполнении самостоятельной работы, обучающемуся необходимо обратиться за консультацией к педагогическому работнику. Периоды проведения консультаций устанавливаются в расписании консультаций.

9 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине "Безопасность операционных систем", включая перечень программного обеспечения и информационных справочных систем

Для изучения дисциплины может использоваться следующее программное обеспечение:
1. Ubuntu
2. Mozilla Firefox
3. Google Chrome
4. 7-zip
5. Microsoft Windows
6. ESET NOD32 Smart Security Business Edition
7. Kaspersky Endpoint Security
8. Браузер Спутник

10 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине "Безопасность операционных систем"

Для реализации программы учебной дисциплины предусмотрены специальные помещения:

1. Помещения для самостоятельной работы обучающихся должны оснащенные компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа к электронной информационно-образовательной среде Организации.

2. Учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

11 Иные сведения и (или) материалы

1. Образовательный процесс осуществляется с использованием как традиционных так и современных интерактивных технологий.

В рамках аудиторных занятий применяются следующие интерактивные методы:

- разбор конкретных примеров;
- мультимедийная презентация.

2. Проведение групповых и индивидуальных консультаций осуществляется в соответствии с расписанием консультаций по темам, заявленным в рабочей программе дисциплины, в период освоения дисциплины и перед промежуточной аттестацией с учетом результатов текущего контроля.