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

Паспорт экзамена

по дисциплине «Безопасность операционных систем», 4 семестр

Методика оценки

Экзамен проводится в устной форме по билетам. Билет состоит из 2 вопросов и формируется по следующему правилу:
первый вопрос выбирается из диапазона вопросов 1–20;
второй вопрос выбирается из диапазона вопросов 21–40.

Таким образом, проверяются результаты обучения по дисциплине, соотнесённые с установленными в программе индикаторами достижения компетенций ОПК-11.3.1, ОПК-12.1 и ОПК-12.3.

На экзамене преподаватель вправе задавать студенту уточняющие и 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. Вопрос 1
2. Вопрос 2.

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

Критерии оценки результатов обучения, соотнесенных с уровнями освоения индикаторов достижения компетенций

Ответ на экзаменационный билет засчитывается на **продвинутом** уровне, если студент проводит сравнительный комплексный анализ материала, выявляет проблемы, предлагает механизмы их решения, представляет количественные характеристики определенных процессов, приводит конкретные примеры, не допускает ошибок. Совокупность результатов обучения по дисциплине и соотнесенных с ними индикаторов достижения компетенций не содержит пробелов. Установленные в программе компетенции сформированы в полном объеме. Оценка составляет *от 35 до 40 баллов.*

Ответ на экзаменационный билет засчитывается на **базовом** уровне, если студент при ответе на вопросы формулирует основные понятия, дает характеристику процессов, явлений, проводит анализ причин, условий, способен представить количественные и качественные характеристики процессов, не допускает существенных ошибок. Совокупность результатов обучения по дисциплине и соотнесенных с ними индикаторов достижения компетенций содержит несущественные пробелы. Установленные в программе компетенции сформированы на базовом уровне. Оценка составляет *от 27 до 34 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, допускает непринципиальные ошибки. Совокупность результатов обучения по дисциплине и соотнесенных с ними индикаторов достижения компетенций содержит пробелы. Установленные в программе компетенции сформированы на пороговом уровне. Оценка составляет *от 20 до 26 баллов.*

Ответ на экзаменационный билет считается **неудовлетворительным** (ниже порогового уровня), если студент при ответе на вопросы не дает определений основных понятий, не способен показать причинно-следственные связи явлений, допускает принципиальные ошибки. Совокупность результатов обучения по дисциплине и соотнесенных с ними индикаторов достижения компетенций содержит существенные пробелы. Установленные в программе компетенции не сформированы. Оценка составляет *менее* 20 *баллов.*

Шкала оценки

Экзамен считается сданным, если сумма баллов по всем заданиям билета составляет от 20 до 40 баллов включительно. Сумма менее 20 баллов признается неудовлетворительным результатом промежуточной аттестации по дисциплине.

В общей оценке по дисциплине экзаменационные баллы учитываются в соответствии с правилами балльно-рейтинговой системы, установленными в НГТУ.

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

1. Назначение операционной системы. Управление ресурсами и предоставление интерфейсов приложениям и пользователю.
2. Архитектуры операционных систем: монолитное ядро, микроядро и модульная организация. Влияние архитектуры на изоляцию компонентов.
3. Пользовательский и привилегированный режимы работы. Системные вызовы и граница защиты ядра.
4. Процесс как объект управления ОС. Состояния процесса, контекст и переключение контекста.
5. Потоки исполнения и их отличие от процессов. Совместное использование ресурсов и вопросы изоляции.
6. Планирование процессов. Приоритеты, вытесняющее планирование и влияние распределения ресурсов на доступность системы.
7. Межпроцессное взаимодействие: каналы, разделяемая память и обмен сообщениями. Контроль доступа к средствам взаимодействия.
8. Синхронизация процессов и потоков. Критическая секция, взаимное исключение и условия возникновения взаимоблокировок.
9. Организация оперативной памяти. Логические и физические адреса, адресное пространство процесса.
10. Виртуальная память и страничная организация. Отображение адресов и обработка отсутствующей страницы.

11. Защита памяти: разделение адресных пространств и права чтения, записи и исполнения страниц.
12. Подкачка и управление памятью. Влияние нехватки памяти на производительность и доступность ОС.
13. Файл как объект ОС. Атрибуты, файловые дескрипторы и основные операции с файлами.
14. Организация каталогов и разрешение путей. Абсолютные и относительные пути, ссылки и особенности контроля доступа.
15. Структура файловой системы. Размещение данных и метаданных, монтирование и проверка состояния файловой системы.
16. Права доступа к файлам и каталогам. Наследование прав и различия между доступом к каталогу и к его содержимому.
17. Назначение подсистемы ввода-вывода. Драйверы, прерывания, буферизация и взаимодействие с ядром.
18. Разделение доступа к устройствам. Риски привилегированных драйверов и защита ресурсов ввода-вывода.
19. Сетевые функции операционной системы. Клиентские и серверные службы, сетевые соединения и общие ресурсы.
20. Сетевые операционные системы. Централизованное управление ресурсами, учётными записями и доступом.
21. Конфиденциальность, целостность и доступность информации применительно к операционной системе.
22. Субъекты и объекты доступа в ОС. Политика безопасности, механизм защиты и доверенная вычислительная база.
23. Типовые угрозы безопасности ОС. Нарушение разграничения доступа, повышение привилегий и нарушение доступности.
24. Защитные механизмы ОС: идентификация, аутентификация, авторизация, регистрация событий и контроль целостности.
25. Принцип минимальных привилегий и разделение административных и пользовательских полномочий.
26. Дискреционное управление доступом. Матрица доступа, владелец объекта, списки управления доступом и их проверка.
27. Мандатное управление доступом. Метки безопасности, уровни доступа и отличия от дискреционной модели.
28. Мандатное управление доступом и контроль целостности. Различие целей защиты конфиденциальности и целостности.
29. Учётные записи пользователей и группы. Идентификаторы, членство и организация группового доступа.
30. Администрирование жизненного цикла учётной записи: создание, изменение полномочий, блокирование и удаление.
31. Основы командной строки Windows. Работа с каталогами и файлами, просмотр справки и параметров команд.
32. Базовое администрирование Windows: просмотр процессов, служб, пользователей и сетевой конфигурации.
33. Основы терминала Linux. Оболочка, команды, конвейеры и перенаправление стандартных потоков.

34. Базовое администрирование Linux: просмотр процессов и служб, управление файлами и правами доступа.
35. Отечественные операционные системы. Назначение Astra Linux и особенности выбора ОС для защищённой автоматизированной системы.
36. Astra Linux: основные компоненты, графическая среда и средства базового администрирования.
37. Базовое администрирование Astra Linux через CLI. Пользователи, группы, файловые права и проверка результата команд.
38. Средства защиты информации Astra Linux. Назначение дискреционного и мандатного разграничения доступа и контроля целостности.
39. Проверка политики доступа в учебной ОС: положительные и отрицательные проверки, фиксация исходного и итогового состояния.
40. Первичные действия при обнаружении нарушения доступа в ОС: фиксация признаков, сохранение сведений о событии и ограничение последствий в пределах полномочий.