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

Паспорт экзамена

по дисциплине «Безопасность операционных систем», 5 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 1–18;
второй вопрос выбирается из диапазона вопросов 19–36.

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. Объекты и цели защиты информации в информационно-вычислительной системе. Роль операционной системы в обеспечении безопасности.
2. Политика безопасности и требования к защите ОС. Соотношение организационных и программно-технических мер.
3. Угрозы конфиденциальности, целостности и доступности в информационно-вычислительных системах.
4. Нарушитель, уязвимость и инцидент безопасности. Условия реализации угроз и определение защищаемых ресурсов.
5. Программно-технический уровень обеспечения безопасности: состав средств защиты и их согласованная настройка.
6. Принципы минимальных привилегий, разделения обязанностей и изоляции при организации защиты ОС.
7. Подсистема безопасности Windows. Основные компоненты и последовательность проверки доступа к объекту.
8. Идентификаторы безопасности SID и маркеры доступа Windows. Связь пользователя, групп и привилегий с доступом процесса.
9. Идентификация и аутентификация в Windows. Локальные и доменные учётные записи, проверка подлинности пользователя.
10. Авторизация в Windows. Дескриптор безопасности, владелец объекта и списки DACL и SACL.

11. Разрешающие и запрещающие записи доступа Windows. Наследование прав и определение эффективного доступа.
12. Привилегии пользователей Windows и объектные разрешения. Различие назначения и ограничения полномочий администратора.
13. Политики безопасности Windows: политика паролей, блокировки учётных записей и назначение прав пользователей.
14. Настройка локальной политики безопасности Windows. Проверка применённых параметров и документирование изменений.
15. Политика аудита Windows. Выбор событий успешного и неуспешного доступа и связь аудита с настройкой SACL.
16. Журналы событий Windows: назначение, отбор событий и анализ попыток входа и изменения прав доступа.
17. Администрирование безопасности Windows средствами PowerShell. Получение сведений о пользователях, группах и разрешениях.
18. PowerShell при анализе событий безопасности: фильтрация, экспорт результатов и проверка корректности административного сценария.
19. Подсистема безопасности UNIX. Учётные записи, идентификаторы UID/GID, группы и привилегированные процессы.
20. Идентификация и аутентификация в UNIX. Учётные данные, ограничения доступа к ним и назначение PAM.
21. Авторизация в UNIX: права rwx для владельца, группы и остальных пользователей; особенности прав каталогов.
22. Расширенные списки доступа ACL и маска ACL в UNIX. Взаимодействие с обычными файловыми правами.
23. Специальные биты доступа setuid, setgid и sticky. Назначение и риски при администрировании UNIX.
24. Привилегии root и делегирование административных действий в UNIX. Контроль использования повышенных полномочий.
25. Подсистема безопасности Astra Linux Special Edition. Сочетание механизмов разграничения доступа и контроля целостности.
26. Идентификация, аутентификация и авторизация в Astra Linux Special Edition. Проверка пользовательского контекста доступа.
27. Дискреционное управление доступом в Astra Linux Special Edition. Настройка прав и контроль результата.
28. Механизм расширения дискреционного управления доступом в Astra Linux Special Edition. Назначение и взаимодействие с базовыми правами.
29. Мандатное управление доступом в Astra Linux Special Edition. Метки субъектов и объектов, проверка разрешённого информационного обмена.
30. Мандатный контроль целостности в Astra Linux Special Edition. Уровни целостности и ограничение воздействия на защищённые объекты.
31. Аудит в UNIX: источники событий, отбор значимых записей и обеспечение сохранности журналов.
32. Подсистема аудита Astra Linux Special Edition. Регистрация доступа и административных изменений, анализ результатов проверки.
33. План проверки подсистемы безопасности ОС: разрешённые и запрещённые действия, контроль ожидаемых результатов и воспроизводимость.

34. Реагирование на инцидент несанкционированного доступа в Windows: сбор исходных сведений, локализация и проверка восстановления защиты.
35. Реагирование на инцидент нарушения прав или меток доступа в UNIX и Astra Linux: сохранение событий и обоснование корректирующих мер.
36. Сравнение подсистем безопасности Windows и Astra Linux Special Edition при проектировании защищённой автоматизированной системы.