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

Паспорт экзамена

по дисциплине «Защита информационных систем», 3 семестр

1. Методика оценки

Экзамен проводится в устной форме, по билетам. Билет формируется по следующему правилу: первый вопрос выбирается из диапазона вопросов 1-20, второй вопрос из диапазона вопросов 21-45 (список вопросов приведен ниже). В ходе экзамена преподаватель вправе задавать студенту дополнительные вопросы из общего перечня (п. 4).

Форма экзаменационного билета

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Факультет АВТФ

Билет № _____
к экзамену по дисциплине «Защита информационных систем»

---

1. Классификация сетевых угроз и атак.
2. Управление ключами.

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

2. **Критерии оценки**

- Ответ на экзаменационный билет считается **неудовлетворительным**, если студент при ответе на вопросы не дает определений основных понятий, не способен показать причинно-следственные связи явлений, при решении задачи допускает принципиальные ошибки, оценка составляет *_10_ 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, при решении задачи допускает непринципиальные ошибки, например, вычислительные, оценка составляет *20 баллов.*
- Ответ на экзаменационный билет билет засчитывается на **базовом** уровне, если студент при ответе на вопросы формулирует основные понятия, законы, дает характеристику

процессов, явлений, проводит анализ причин, условий, может представить качественные характеристики процессов, не допускает ошибок при решении задачи, оценка составляет *_30_ баллов.*

- Ответ на экзаменационный билет билет засчитывается на **продвинутом** уровне, если студент при ответе на вопросы проводит сравнительный анализ подходов, проводит комплексный анализ, выявляет проблемы, предлагает механизмы решения, способен представить количественные характеристики определенных процессов, приводит конкретные примеры из практики, не допускает ошибок и способен обосновать выбор метода решения задачи, оценка составляет _40_ *баллов.*

3. Шкала оценки

В общей оценке по дисциплине экзаменационные баллы учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

4. **Вопросы к** экзамену **по дисциплине «**Защита информационных систем**»**

1. Классификация компьютерных сетей.
2. Функциональная иерархическая модель информационных сетей.
3. Общая характеристика распределенной операционной системы.
4. Функции и основные характеристики корпоративных сетей.
5. Типовая структура корпоративной компьютерной сети.
6. Фазы процесса связи удаленных объектов.
7. Классификация сетевых угроз и атак.
8. Рекомендации по построению систем защиты.
9. Межсетевые экраны (МЭ) с фильтрацией пакетов.
10. Межсетевые экраны уровня приложений.
11. Шлюзы уровня соединений.
12. МЭ с адаптивной проверкой пакетов (или МЭ с запоминанием состояния пакетов).
13. Способы НСД к информации.
14. Методы и средства защиты от НСД в сети.
15. Аутентификация пользователей.
16. Основные особенности сетевой аутентификации.
17. Простой метод запрос-ответ.
18. Аутентификация в протоколе SMB (Server Message Block – блок сообщений сервера).
19. Разграничение доступа пользователей к ресурсам АС.
20. Криптографические сетевые протоколы.
21. Протокол IPSec.
22. Протокол TLS.
23. Стандарт SET.
24. Управление ключами.
25. KDC.
26. Система распределенной аутентификации Kerberos.
27. Стандарты безопасности вычислительных сетей и их компонентов.
28. Классификация СВТ по уровню защищенности от НСД.
29. Классификация автоматизированных систем по уровню защищенности от НСД.
30. Межсетевые экраны. Показатели защищенности от НСД к информации.
31. Базовые протоколы семейства TCP/IP.
32. Прикладной уровень TCP/IP.
33. Транспортный уровень TCP/IP.
34. Межсетевой уровень TCP/IP.
35. Уровень доступа к сети.

36. Прикладные протоколы и службы (WWW, электронная почта, передача файлов).
37. Виртуальные частные сети.
38. Построение VPN на базе сетевой операционной системы.
39. Построение VPN на базе маршрутизаторов.
40. Построение VPN на базе межсетевых экранов.
41. Вопросы безопасности базовых протоколов TCP/IP.
42. Перехват данных, имперсонация, отказ в обслуживании.
43. Несанкционированное подключение к сети.
44. Несанкционированный обмен данными.
45. Безопасность WWW, электронной почты, Java.