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

Паспорт зачета

по дисциплине «Безопасность сетей электронных вычислительных машин», 6 семестр

1. Методика оценки

Зачет проводится в устной форме, по билетам. Билет состоит из 2 вопросов и формируется по следующему правилу:

- первый вопрос выбирается из диапазона вопросов 1 – 33;
- второй вопрос из диапазона вопросов 34 – 66.

Таким образом, проверяются результаты обучения по дисциплине, соотнесенные с установленными в программе индикаторами достижения компетенций.

На зачете преподаватель вправе задавать студенту уточняющие и дополнительные вопросы из общего перечня (п. 4).

Форма билета для зачета

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Факультет АВТФ

Билет № _____
к зачету по дисциплине «Безопасность сетей электронных вычислительных машин»

1. Вопрос 1.
2. Вопрос 2.

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

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

Ответ на билет для зачета 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. 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* 18 *до* 20 *баллов.*

Ответ на билет для зачета 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. 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* 14 *до* 17 *баллов.*

Ответ на билет для зачета засчитывается на **пороговом** уровне, если студент при ответе на вопросы дает определение основных понятий, может показать причинно-следственные связи явлений. 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* 10 *до* 13 *баллов.*

Ответ на билет для зачета считается **неудовлетворительным** (ниже порогового уровня), если студент при ответе на вопросы не дает определений основных понятий, не способен показать причинно-следственные связи явлений. Совокупность результатов обучения по дисциплине и соотнесенных с ними индикаторов достижения компетенций содержит существенные пробелы. Установленные в программе компетенции не сформированы. Оценка составляет *менее* 10 *баллов.*

3. Шкала оценки

Зачет считается сданным, если сумма баллов по всем заданиям билета составляет от 10 до 20 баллов включительно. Сумма менее 10 баллов признается неудовлетворительным результатом промежуточной аттестации по дисциплине.

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

4. Вопросы к зачету по дисциплине «Безопасность сетей электронных вычислительных машин»

1. Анализ угроз информационной безопасности. Классификация угроз безопасности в информационных системах.
2. Угрозы несанкционированного доступа к информации в информационной системе.
3. Характеристика источников угроз несанкционированного доступа в информационной системе и результатов несанкционированного или случайного доступа.
4. Характеристика уязвимостей информационной системы. Уязвимости отдельных протоколов стека протоколов TCP/IP.
5. Характеристика угроз безопасности, реализуемых с использованием протоколов межсетевого взаимодействия. Классификационная схема угроз. Первичные признаки классификации. Назвать наиболее часто реализуемых в настоящее время угрозы.
6. Угроза «Анализ сетевого трафика». Сканирование сети. Угроза выявления пароля. Отказ в обслуживании.
7. Подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа.
8. Навязывание ложного маршрута сети.
9. Внедрение ложного объекта сети.

10. Удаленный запуск приложений
11. Модели безопасности компьютерных систем. Модели дискреционного разграничения доступа.
12. Модели безопасности компьютерных систем. Модели мандатного разграничения доступа.
13. Модели безопасности компьютерных систем. Модели ролевого разграничения доступа.
14. Модели безопасности компьютерных систем. Модели безопасности информационных потоков.
15. Модели безопасности компьютерных систем. Субъектно ориентированная модель изолированной программной среды.
16. Идентификация, аутентификация и управление доступом. Аутентификация, авторизация и администрирование действий пользователей.
17. Биометрическая идентификация и аутентификация. Обобщенная биометрическая система. Функции обобщенной биометрической системы.
18. Биометрические профили для взаимодействия и обмена данными. Общая архитектура биометрической системы и биометрические профили информационной безопасностью. ГОСТ ISO/IEC 24713-1-2013.
19. Вопросы обеспечения безопасности в операционной среде Windows. Аутентификация пользователей при удаленном доступе.
20. Механизм идентификации и аутентификации в ОС Windows. Процесс Winlogon.
21. Механизм идентификации и аутентификации в ОС Windows. Локальная аутентификация пользователя в Windows.
22. Механизм идентификации и аутентификации в ОС Windows. Сетевая аутентификация пользователя в Windows.
23. Механизм идентификации и аутентификации в ОС Windows. Макет системы защиты от несанкционированного доступа.
24. Протокол сервиса Каталога LDAP (Lightweight Directory Access Protocol).
25. Служба каталогов Active Directory. Архитектура AD, стратегия именования объектов и планирование инфраструктуры.
26. Инфраструктуры открытых ключей. Доверие в сфере электронных коммуникаций.
27. Инфраструктуры открытых ключей. Концепция инфраструктуры безопасности
28. Инфраструктуры открытых ключей. Цель и сервисы инфраструктуры безопасности.
29. Инфраструктуры открытых ключей. Механизмы аутентификации
30. Инфраструктуры открытых ключей. Основные компоненты PKI.
31. Инфраструктуры открытых ключей. Основные сервисы PKI.
32. Инфраструктуры открытых ключей. Сервисы безопасности PKI
33. Инфраструктуры открытых ключей. Модели и механизмы доверия
34. Инфраструктуры открытых ключей. Сертификаты открытых ключей.
35. Классификация сертификатов и управление ими.
36. Инфраструктуры открытых ключей. Основные понятия архитектуры PKI.
37. Инфраструктуры открытых ключей. Механизмы распространения информации PKI
38. Инфраструктуры открытых ключей. Политики, регламент и процедуры PKI. Политика безопасности и способы ее реализации.
39. Инфраструктуры открытых ключей. Сервисы, базирующиеся на PKI. Механизмы необходимые для сервисов. Условия функционирования сервисов.
40. Инфраструктуры открытых ключей. Приложения, базирующиеся на PKI. Защищенная электронная почта S/MIME.
41. Инфраструктуры открытых ключей. Приложения, базирующиеся на PKI. Средства безопасности транспортного уровня.
42. Инфраструктуры открытых ключей. Приложения, базирующиеся на PKI. Средства

безопасности IP-уровня.

43. Инфраструктуры открытых ключей. Приложения, базирующиеся на PKI. Типовые сценарии использования PKI.
44. Протоколы безопасного сетевого взаимодействия. Протоколы сетевой аутентификации.
45. Протоколы безопасного сетевого взаимодействия. Протокол Kerberos.
46. Протоколы защищенных каналов. Защита на канальном уровне - протоколы PPTP и L2TP.
47. Протоколы защищенных каналов. Защита на сетевом уровне - протокол IPSec.
48. Протоколы защищенных каналов. Защита на сеансовом уровне - протоколы SSL, TLS и SOCKS.
49. Протоколы защищенных каналов. Протокол SSH.
50. Протоколы защищенных каналов. Защита беспроводных сетей.
51. Технологии межсетевых экранов. Функции межсетевых экранов.
52. Технологии межсетевых экранов. Особенности функционирования межсетевых экранов на различных уровнях модели OSI
53. Технологии межсетевых экранов. Схемы сетевой защиты на базе межсетевых экранов.
54. Технологии виртуальных защищенных сетей VPN. Концепция построения виртуальных защищенных сетей VPN. Классификация VPN.
55. Технологии виртуальных защищенных сетей VPN. VPN-решения для построения защищенных сетей.
56. Технологии виртуальных защищенных сетей VPN. Основные виды технической реализации VPN.
57. Защита удаленного доступа. Централизованный контроль удаленного доступа. Протоколы TACACS и RADIUS.
58. Технологии обнаружения и предотвращения вторжений.
59. Принципы многоуровневой защиты корпоративной информации.
60. Корпоративная информационная система с традиционной структурой.
61. Многоуровневый подход к обеспечению информационной безопасности КИС.
62. Подсистемы информационной безопасности традиционных КИС.
63. Безопасность «облачных» вычислений.
64. Основные проблемы безопасности «облачной» инфраструктуры.
65. Средство защиты в виртуальных средах.
66. Безопасность промышленных систем и АСУ ТП.