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

Паспорт зачета

по дисциплине «Программно-аппаратные средства обеспечения информационной безопасности», 6 семестр

1. Методика оценки

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

- первый вопрос выбирается из диапазона вопросов 1-21;
- второй вопрос из диапазона вопросов 22-41.

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 «Программно-аппаратные средства обеспечения информационной безопасности»

---

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, не допускает ошибок. Совокупность результатов обучения по дисциплине (модулю) 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 (модулю) 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 (модулю) 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 (модулю) 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 «**Программно-аппаратные средства обеспечения информационной безопасности**»**

1. Какие основные нормативные документы регулируют информационную безопасность в Российской Федерации?
2. Что такое ФСТЭК и какие функции выполняет эта организация?
3. Какие требования предъявляются к программно-аппаратным средствам защиты информации согласно российскому законодательству?
4. Что такое сертифицированные средства защиты информации и зачем нужна сертификация?
5. Какие уровни/классы защищенности информационных систем существуют и как они определяются?
6. Что такое несанкционированный доступ к информации и какие виды НСД существуют?
7. Какие методы аутентификации пользователей вы знаете?
8. Что такое мандатный и дискреционный контроль доступа?
9. Как работает система разграничения прав доступа на основе ролей (RBAC)?
10. Что такое идентификация и аутентификация? В чем разница между этими понятиями?
11. Какие средства защиты от НСД применяются на уровне операционной системы?

12. Что такое политики безопасности и как они реализуются в информационных системах?
13. Что такое межсетевой экран и какие основные функции он выполняет?
14. Какие типы межсетевых экранов существуют?
15. Что такое многофункциональный межсетевой экран (NGFW) и чем он отличается от традиционного?
16. Что такое межсетевой экран уровня веб-приложений (WAF) и какие угрозы он предотвращает?
17. Какие правила фильтрации трафика можно настроить на межсетевом экране?
18. Что такое IDS и IPS? В чем разница между этими системами?
19. Какие методы обнаружения вторжений существуют?
20. Как работает система обнаружения вторжений на основе анализа аномалий?
21. Что такое ложные срабатывания в системах обнаружения вторжений и как их минимизировать?
22. Где размещаются IDS/IPS в сетевой инфраструктуре и какие режимы работы они поддерживают?
23. Какие основные задачи решает криптографическая защита информации?
24. Что такое симметричное и асимметричное шифрование?
25. Что такое электронная подпись и как она работает?
26. Какие виды электронных подписей существуют?
27. Что такое хеш-функция и для чего она используется в криптографии?
28. Как работает инфраструктура открытых ключей (PKI)?
29. Какие методы обнаружения вредоносного программного обеспечения существуют?
30. Какие типы вредоносного ПО вы знаете?
31. Как работает песочница (sandbox) в системах антивирусной защиты?
32. Что такое уязвимость информационной системы и какие типы уязвимостей существуют?
33. Как работают сканеры уязвимостей и какие методы сканирования они используют?
34. Что такое CVE и CVSS? Как оценивается критичность уязвимостей?
35. Какие этапы включает процесс управления уязвимостями?
36. Чем отличается активное сканирование от пассивного анализа уязвимостей?
37. Что такое SIEM-система и какие задачи она решает?
38. Какие основные компоненты входят в архитектуру SIEM-системы?
39. Что такое SOC (Security Operations Center) и какие функции он выполняет?
40. Как происходит сбор и корреляция событий безопасности в SIEM-системах?
41. Что такое инцидент информационной безопасности и как организуется реагирование на инциденты в SOC?