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

Паспорт зачета

по дисциплине «Проектирование доверенных информационных систем», 10 семестр

1. Методика оценки

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

- первый вопрос выбирается из диапазона вопросов 1-20;
- второй вопрос из диапазона вопросов 21-43.

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 «Проектирование доверенных информационных систем»

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 (тест) 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 (тест) 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 (тест) 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 (тест) 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 «**Проектирование доверенных информационных систем**»**

1. Что такое «доверие» в контексте информационной безопасности? Дайте определение.
2. Чем понятие «доверие» отличается от понятия «безопасность» в ИТ-системах?
3. Какие факторы влияют на уровень доверия к информационной системе?
4. Что включает в себя модель обеспечения доверия к ИТ-продукту?
5. Какие этапы жизненного цикла ИТ-системы влияют на обеспечение доверия?
6. Как концепция доверия интегрируется в процесс разработки защищённых систем?
7. Какие международные и российские стандарты регулируют вопросы обеспечения доверия к ИТ-системам?
8. Чем различаются подходы к оценке доверия в стандартах Common Criteria и отечественных нормативных документах?
9. Что представляет собой стандарт ИСО/МЭК 15408 (Common Criteria)?
10. Какова структура Common Criteria (части стандарта)?
11. Что такое профиль защиты (Protection Profile) и целевой объект оценки (TOE)?
12. Кто является участниками процесса оценки по Common Criteria?
13. Что такое функциональные требования безопасности в модели Common Criteria?
14. Какие классы функциональных требований безопасности существуют?
15. Что такое пакет функциональных требований и как он формируется?
16. Приведите примеры функциональных требований к управлению доступом и аудиту.

17. Что такое оценочный уровень доверия (Evaluation Assurance Level, EAL)?
18. Сколько уровней EAL существует и чем они отличаются друг от друга?
19. Какие механизмы управления доступом предусмотрены в функциональных требованиях безопасности?
20. Какие методы аутентификации пользователей рассматриваются в контексте доверенных систем?
21. Что такое политика управления доступом (FDP_ACC, FDP_ACF) в терминах Common Criteria?
22. Какие требования предъявляются к подсистеме аудита безопасности (FAU класс)?
23. Как криптографические механизмы обеспечивают доверие к ИТ-системе?
24. Какие требования безопасности предъявляются к защищённой связи между компонентами системы?
25. Что включает в себя управление безопасностью (FMT класс) в модели Common Criteria?
26. Как обеспечивается приватность (конфиденциальность персональных данных) в доверенных системах?
27. Какие роли и привилегии предусмотрены в механизмах управления безопасностью?
28. Что такое защита функциональных возможностей безопасности (FPT класс)?
29. Как обеспечивается целостность самих механизмов безопасности в доверенной системе?
30. Что означает требование самозащиты (self-protection) для TOE?
31. Что оценивается в классе ADV (Разработка) по Common Criteria?
32. Какие требования предъявляются к архитектуре безопасности и внутреннему устройству TOE?
33. Что такое формальная модель политики безопасности и когда она требуется?
34. Что оценивается в классе ALC (Поддержка жизненного цикла)?
35. Какие требования предъявляются к конфигурационному управлению и процедуре поставки TOE?
36. Почему безопасная разработка и контроль версий важны для обеспечения доверия?
37. Что оценивается в классе AGD (Руководства) и классе ATE (Тестирование)?
38. Какие требования предъявляются к пользовательской и администраторской документации?
39. Какие виды тестирования проводятся при оценке доверия (функциональное, независимое, глубокое)?
40. Что оценивается в классе AVA (Анализ уязвимостей)?
41. Какие виды анализа уязвимостей проводятся на разных уровнях EAL?
42. Что такое композиция (ACO) и как оценивается безопасность составных систем?
43. Какие особенности имеет оценка доверия автоматизированных систем управления (АСУ)?