Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»
Кафедра экономической информатики

Паспорт зачета

по дисциплине «Информационная безопасность и защита информации», 7 семестр

1. Методика оценки

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

- первый вопрос выбирается из диапазона вопросов 1 – 45;
- второй вопрос из диапазона вопросов 46 – 65.

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 ФБ

Билет № 1
к зачету по дисциплине «Информационная безопасность и защита информации»

1. Защищаемая информация: банковская тайна и государственная тайна. Определение, основные принципы регулирования, ответственность.
2. Виды хакерских атак.

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 дисциплинеи 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, 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* 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, допускает непринципиальные ошибки, например, вычислительные. 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 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 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 «Информационная безопасность и защита информации»

1. Информационная безопасность - определение. Ключевые принципы. ИБ как состояние.
2. Структура правового регулирования ИБ в РФ.
3. Регулирующие и надзорные органы в сфере защиты информации в России. Их основные функции и задачи.
4. БДУ ФСТЭК России. Описание, назначение, сферы применения.
5. Методика оценки рисков. Формирование матрицы рисков и стратегии противодействия.
6. Защищаемая информация: персональные данные и врачебная тайна. Определение, основные принципы регулирования, ответственность.
7. Защищаемая информация: банковская тайна и государственная тайна. Определение, основные принципы регулирования, ответственность.
8. Персональные данные: практика регулирования в России и в Евросоюзе. Различия, сходство.
9. Уголовный Кодекс РФ, КоАП РФ и преступления \ правонарушения в области защиты информации: диспозиция и санкции.
10. ИСПДн: определение, обязанности оператора, регулирование мер защиты.

11. Классы защищенности ИСПДн и порядок их присвоения.
12. Порядок оценки угроз ИБ по методике ФСТЭК
13. ISO27001: стадии построения СУИБ и их краткое описание
14. Модель нарушителя и модель угроз. Определение, пример построения.
15. ЭЦП. Определение, примеры применения в РФ. Законодательные акты, правовое регулирование и примеры их применения.
16. Криптографическая защита: определение, история, примеры применения
17. Криптографическая защита: правовое регулирование в России
18. Соглашение о конфиденциальности. Определение, назначение, порядок работы.
19. Коммерческая тайна. определение, порядок внедрения.
20. Система ограничительных грифов. Определение, примеры грифов, обязанности получателя документа.
21. Биометрические данные. Определение, примеры, особенности сбора и обработки
22. Что такое непрерывность бизнеса? Инциденты, их отличия от рисков.
23. Стадии расследования инцидента - какие действия следует предпринять.
24. Способы обнаружения инцидентов и свойства реакции на них
25. Виды инцидентов и примеры (согласно ГОСТ)
26. Классификация информации. Виды данных и носителей.
27. Ценность информации. Цена информации.
28. Количество и качество информации.
29. Виды защищаемой информации.
30. Классификация источников и носителей информации.
31. Криптовалюты и информационная безопасность.
32. Информационная безопасность промышленных сетей и предприятий.
33. Безопасность радиосвязи: наводки. паразитные сигналы.
34. Персональные данные как средство отслеживания субъекта.
35. Парольная защита и средства ее обхода.
36. Безопасность в облачных системах в сети Интернет.
37. Мошенничество с использованием современных технологий.
38. Методы несанкционированного доступа к информации.
39. Безопасность в государственных учреждениях в России.
40. Способы наблюдения с использованием технических средств.
41. Каналы утечки информации.
42. Безопасность беспроводных сетей связи (WiFi, WiMax).
43. Безопасность в сетях мобильной связи (GSM).
44. Технологии скрытого видеонаблюдения и правовые последствия.
45. Система защиты сетей связи КНР "Золотой щит".
46. Криптография в современных системах.
47. Понятия скрытия информации, виды скрытий. Стеганография.
48. Антивирусная защита.
49. Компьютерные вирусы.
50. Социальная инженерия в информационной безопасности.
51. Виды хакерских атак.
52. Комплексные решения защиты информации: Positive Technologies, SolarWinds.
53. Средства идентификации личности. Биометрическая защита.
54. Технологии инфильтрации нарушителей в информационные системы.
55. Современные системы видеонаблюдения.
56. Программы Bug Bounty.
57. Защита банковских документов в финансовых учреждениях.
58. Защита государственной тайны в России.
59. Авторизация, аутентификация, идентификация. Многофакторность. История.
60. Информацияонная безопасность в интернете вещей.

61. Военные стандарты кибербезопасности. Кибервойна.
62. Сертификация в области информационной безопасности.
63. Резервное копирование. Принципы и средства.
64. Способы удаленного извлечения информации с компьютера.
65. История носителей информации. Категорирование с точки зрения безопасности.