МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение
высшего образования

«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

ПОДПИСАНО ЭП КУЗГТУ

Директор

Дата: 25.11.2022 12:11:00

..

Фонд оценочных средств дисциплины

Прогнозирование рисков в информационной безопасности

Направление подготовки 10.04.01 Информационная безопасность
Направленность (профиль) Организация и технология защиты информации

Присваиваемая квалификация
"Магистр"

Формы обучения
очно-заочная

5.1 Паспорт фонда оценочных средств

Планируемые результаты обучения по дисциплине (модулю)

Дисциплина направлена на формирование следующих компетенций выпускника:

Форма (ы) текущего контроля	Компетенции, формируемые в результате освоения дисциплины (модуля)	Индикатор (ы) достижения компетенции	Результаты обучения по дисциплине (модулю)	Уровень
Опрос по контрольным вопросам, подготовка отчетов по практическим и (или) лабораторным работам	ПК-7	Анализирует и прогнозирует риски в информационной безопасности и управляет инцидентами информационной безопасности	Знать основные положения, понятия и категории, теоретические основы прогнозирования рисков информационной безопасности; предпосылки для управления информационными рисками; основные требования по управлению рисками информационной безопасности; состав системы управления информационными рисками; порядок оценки рисков информационной безопасности; порядок обработки рисков информационной безопасности; основные методы и технологию управления службой защиты информации. Уметь использовать стандарты в области управления рисками информационной безопасности; осуществлять оценку рисков информационной безопасности; осуществлять обработку результатов оценки рисков информационной безопасности; применять программное обеспечение для оценки рисков информационной безопасности. Владеть навыками оценки угроз безопасности информации в технологии оценки рисков; навыками подбора инструментальных средств для управления информационными рисками.	Высокий или средний
<p>Высокий уровень достижения компетенции - компетенция сформирована частично, рекомендованные оценки: отлично, хорошо, зачтено.</p> <p>Средний уровень достижения компетенции - компетенция сформирована частично, рекомендованные оценки: хорошо, удовлетворительно, зачтено.</p> <p>Низкий уровень достижения компетенции - компетенция не сформирована частично, оценивается неудовлетворительно или не зачтено.</p>				

5.2. Контрольные задания или иные материалы

Текущий контроль успеваемости и аттестационные испытания обучающихся могут быть организованы с использованием ресурсов ЭИОС КузГТУ. Полный перечень оценочных материалов расположен в ЭИОС КузГТУ.: <https://el.kuzstu.ru/login/index.php>.

Текущий контроль успеваемости и аттестационные испытания могут проводиться в письменной и (или) устной, и (или) электронной форме.

5.2.1. Оценочные средства при текущем контроле

Текущий контроль по темам дисциплины заключается в опросе обучающихся по контрольным вопросам в оформлении отчетов по лабораторным работам.

Опросе обучающихся по контрольным вопросам

Обучающийся отвечает на 2 вопроса.

Например:

1. Понятие аудита безопасности
2. Методы анализа данных при аудите ИБ

Критерии оценивания при ответе на вопросы:

- 100 баллов – при правильном и полном ответе на два вопроса;
- 85...99 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 75...84 баллов – при правильном и неполном ответе на два вопроса;
- 65...74 баллов – правильном и полном ответе только на один из вопросов
- 25...64 – при правильном и неполном ответе только на один из вопросов;
- 0...24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-64	65-100
Шкала оценивания	Не зачтено	Зачтено

Примерный перечень контрольных вопросов:

Раздел 1 Аудит информационной безопасности

1. Понятие аудита безопасности
2. Методы анализа данных при аудите ИБ
3. Анализ информационных рисков предприятия
4. Методы оценивания информационных рисков
5. Стандарт «Критерии оценки надежности компьютерных систем» (Оранжевая книга)
6. Гармонизированные критерии Европейских стран
7. Германский стандарт BSI
8. Британский стандарт BS 7799
9. Международный стандарт ISO 17799
10. Международный стандарт ISO 15408 «Общие критерии»
11. Стандарт COBIT
12. Стандарты по безопасности информационных технологий в России
13. Основные понятия ОК
14. Методология оценки безопасности информационных технологий по ОК
15. Оценка уровня доверия функциональной безопасности информационной технологии
16. Обзор классов и семейств ОК
17. Назначение стандарта ISO 17799 для управления информационной безопасностью
18. Практика прохождения аудита и получения сертификата ISO 17799
19. Анализ видов используемых программных продуктов
20. Система CRAMM
21. Система КОНДОР
22. Сетевые сканеры
23. Задачи и содержание работ при проведении аудита ИБ
24. Подготовка предприятия к проведению аудита ИБ
25. Планирование процедуры аудита ИБ
26. Организация и проведение работ по аудиту
27. Алгоритм проведения аудита безопасности предприятия
28. Перечень и систематизация данных, необходимых для проведения аудита ИБ
29. Выработка рекомендаций и подготовка отчетных документов
30. Экономическая оценка обеспечения ИБ

Раздел 2 Методы анализа рисков ИБ

1. Информационная безопасность бизнеса.
2. Развитие службы информационной безопасности.
3. Международная практика защиты информации.
4. Модель Symantec LifeCycle Security.
5. Постановка задачи анализа рисков.
6. Модель Gartner Group.
7. Модель Carnegie Mellon University.
8. Различные взгляды на защиту информации.
9. Национальные особенности защиты информации.
10. Особенности отечественных нормативных документов.

11. Учет остаточных рисков.
12. Международный стандарт ISO 17799.
13. Обзор стандарта BS 7799.
14. Развитие стандарта BS 7799 (ISO 17799).
15. Сравнение стандартов ISO 17799 и BSI.
16. Стандарт США NIST 800-30.
17. Алгоритм описания информационной системы.
18. Идентификация угроз и уязвимостей. Организация защиты информации.
19. Ведомственные и корпоративные стандарты управления ИБ.
20. XBSS-спецификации сервисов безопасности X/Open.
21. Стандарт NASA «Безопасность информационных технологий».
22. Концепция управления рисками MITRE.
23. Вопросы анализа рисков и управления ими.
24. Идентификация рисков.
25. Оценивание рисков.
26. Измерение рисков.
27. Выбор допустимого уровня риска.
28. Выбор контрмер и оценка их эффективности.
29. Разработка корпоративной методика анализа рисков.
30. Постановка задачи.
31. Методы оценивания информационных рисков.
32. Табличные методы оценки рисков.
33. Методика анализа рисков Microsoft.

Отчеты по лабораторным и (или) практическим работам (далее вместе - работы):

По каждой работе обучающиеся самостоятельно оформляют отчеты в электронном формате (согласно перечню лабораторных и(или) практических работ п.4 рабочей программы).

Содержание отчета:

1. Тема работы.
2. Задачи работы.
3. Краткое описание хода выполнения работы.
4. Ответы на задания или полученные результаты по окончании выполнения работы (в зависимости от задач, поставленных в п. 2).
5. Выводы

Критерии оценивания:

- 75 - 100 баллов - при раскрытии всех разделов в полном объеме

- 0 - 74 баллов - при раскрытии не всех разделов, либо при оформлении разделов в неполном объеме.

Количество баллов	0-74	75-100
Шкала оценивания	Не зачтено	Зачтено

5.2.2 Оценочные средства при промежуточной аттестации

Формами промежуточной аттестации является зачет, в процессе которого определяется сформированность обозначенных в рабочей программе компетенций.

Инструментом измерения сформированности компетенций являются:

- ответы на вопросы во время опроса по разделам дисциплины.
- зачтенные отчеты обучающихся по лабораторным и(или) практическим работам;

На зачете обучающийся отвечает на 2 вопроса.

Критерии оценивания при ответе на вопросы:

- 100 баллов - при правильном и полном ответе на два вопроса;
- 85...99 баллов - при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 75...84 баллов - при правильном и неполном ответе на два вопроса;
- 65...74 баллов - правильном и полном ответе только на один из вопросов
- 25...64 - при правильном и неполном ответе только на один из вопросов;
- 0...24 баллов - при отсутствии правильных ответов на вопросы.

Количество баллов	0-24	25-64	65-74	85-99	100
Шкала оценивания	Неуд		Хорошо	Отлично	
Шкала оценивания	Не зачтено		Зачтено		

Примерный перечень вопросов на зачете:

1. XBSS-спецификации сервисов безопасности X/Open.
2. Алгоритм описания информационной системы.
3. Алгоритм проведения аудита безопасности предприятия
4. Анализ видов используемых программных продуктов
5. Анализ информационных рисков предприятия
6. Британский стандарт BS 7799
7. Ведомственные и корпоративные стандарты управления ИБ.
8. Вопросы анализа рисков и управления ими.
9. Выбор допустимого уровня риска.
10. Выбор контрмер и оценка их эффективности.
11. Выработка рекомендаций и подготовка отчетных документов
12. Гармонизированные критерии Европейских стран
13. Германский стандарт BSI
14. Задачи и содержание работ при проведении аудита ИБ
15. Идентификация рисков.
16. Идентификация угроз и уязвимостей. Организация защиты информации.
17. Измерение рисков.
18. Информационная безопасность бизнеса.
19. Концепция управления рисками MITRE.
20. Международная практика защиты информации.
21. Международный стандарт ISO 15408 «Общие критерии»
22. Международный стандарт ISO 17799
23. Международный стандарт ISO 17799.
24. Методика анализа рисков Microsoft.
25. Методология оценки безопасности информационных технологий по ОК
26. Методы анализа данных при аудите ИБ
27. Методы оценивания информационных рисков
28. Методы оценивания информационных рисков.
29. Модель Carnegie Mellon University.
30. Модель Gartner Group.
31. Модель Symantec LifeCycle Security.
32. Назначение стандарта ISO 17799 для управления информационной безопасностью
33. Национальные особенности защиты информации.
34. Обзор классов и семейств ОК
35. Обзор стандарта BS 7799.
36. Организация и проведение работ по аудиту
37. Основные понятия ОК
38. Особенности отечественных нормативных документов.
39. Оценивание рисков.
40. Оценка уровня доверия функциональной безопасности информационной технологии
41. Перечень и систематизация данных, необходимых для проведения аудита ИБ
42. Планирование процедуры аудита ИБ
43. Подготовка предприятия к проведению аудита ИБ
44. Понятие аудита безопасности
45. Постановка задачи анализа рисков.
46. Постановка задачи.
47. Практика прохождения аудита и получения сертификата ISO 17799
48. Развитие службы информационной безопасности.
49. Развитие стандарта BS 7799 (ISO 17799).
50. Различные взгляды на защиту информации.
51. Разработка корпоративной методики анализа рисков.
52. Сетевые сканеры
53. Система CRAMM
54. Система КОНДОР
55. Сравнение стандартов ISO 17799 и BSI.
56. Стандарт «Критерии оценки надежности компьютерных систем» (Оранжевая книга)
57. Стандарт NASA «Безопасность информационных технологий».
58. Стандарт COBIT
59. Стандарт США NIST 800-30.

60. Стандарты по безопасности информационных технологий в России
61. Табличные методы оценки рисков.
62. Учет остаточных рисков.
63. Экономическая оценка обеспечения ИБ

2.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций

1. Текущий контроль успеваемости обучающихся, осуществляется в следующем порядке: в конце завершения освоения соответствующей темы обучающиеся, по распоряжению педагогического работника, убирают все личные вещи, электронные средства связи и печатные источники информации.

Для подготовки ответов на вопросы обучающиеся используют чистый лист бумаги любого размера и ручку. На листе бумаги обучающиеся указывают свои фамилию, имя, отчество (при наличии), номер учебной группы и дату проведения текущего контроля успеваемости.

Научно-педагогический работник устно задает два вопроса, которые обучающийся может записать на подготовленный для ответа лист бумаги.

В течение установленного научно-педагогическим работником времени обучающиеся письменно формулируют ответы на заданные вопросы. По истечении указанного времени листы бумаги с подготовленными ответами обучающиеся передают научно-педагогическому работнику для последующего оценивания результатов текущего контроля успеваемости.

При подготовке ответов на вопросы обучающимся запрещается использование любых электронных и печатных источников информации. В случае обнаружения научно-педагогическим работником факта использования обучающимся при подготовке ответов на вопросы указанные источники информации – оценка результатов текущего контроля соответствует 0 баллов и назначается дата повторного прохождения текущего контроля успеваемости.

Текущий контроль успеваемости обучающихся по результатам выполнения лабораторных и (или) практических работ осуществляется в форме отчета, который предоставляется научно-педагогическому работнику на бумажном и (или) электронном носителе. Научно-педагогический работник, после проведения оценочных процедур, имеет право вернуть обучающемуся отчет для последующей корректировки с указанием перечня несоответствий. Обучающийся обязан устранить все указанные несоответствия и направить отчет научно-педагогическому работнику в срок, не превышающий трех учебных дней, следующих за днем проведения текущего контроля успеваемости.

Результаты текущего контроля доводятся до сведения обучающихся в течение трех учебных дней, следующих за днем проведения текущего контроля успеваемости.

Обучающиеся, которые не прошли текущий контроль успеваемости в установленные сроки, обязаны пройти его в срок до начала процедуры промежуточной аттестации по дисциплине в соответствии с расписанием промежуточной аттестации.

Результаты прохождения процедур текущего контроля успеваемости обучающихся учитываются при оценивании результатов промежуточной аттестации обучающихся.

1. Промежуточная аттестация обучающихся проводится после завершения обучения по дисциплине в семестре в соответствии с календарным учебным графиком и расписанием промежуточной аттестации.

Для успешного прохождения процедуры промежуточной аттестации по дисциплине обучающиеся должны:

1. получить положительные результаты по всем предусмотренным рабочей программой формам текущего контроля успеваемости;
2. получить положительные результаты аттестационного испытания.

Для успешного прохождения аттестационного испытания обучающийся в течение времени, установленного научно-педагогическим работником, осуществляет подготовку ответов на два вопроса, выбранных в случайном порядке.

Для подготовки ответов используется чистый лист бумаги и ручка.

На листе бумаги обучающиеся указывают свои фамилию, имя, отчество (при наличии), номер учебной группы и дату проведения аттестационного испытания.

При подготовке ответов на вопросы обучающимся запрещается использование любых электронных и печатных источников информации.

По истечении указанного времени, листы с подготовленными ответами на вопросы обучающиеся

передают научно-педагогическому работнику для последующего оценивания результатов промежуточной аттестации.

В случае обнаружения научно-педагогическим работником факта использования обучающимся при подготовке ответов на вопросы указанные источники информации - оценка результатов промежуточной аттестации соответствует 0 баллов и назначается дата повторного прохождения аттестационного испытания.

Результаты промежуточной аттестации обучающихся размещаются в ЭИОС КузГТУ.

Текущий контроль успеваемости и промежуточная аттестация обучающихся могут быть организованы с использованием ЭИОС КузГТУ, порядок и формы проведения текущего контроля успеваемости и промежуточной аттестации обучающихся при этом не меняется.