

МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение
высшего образования

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

Институт информационных технологий, машиностроения и автотранспорта

ПОДПИСАНО ЭП КУЗГТУ

Институт информационных технологий,
машиностроения и автотранспорта
Директор

Дата: 29.09.2026 Н24:45:21

Д.М. Дубинкин

Фонд оценочных средств дисциплины

Основы информационной безопасности и защита данных

Направление подготовки 09.04.04 Программная инженерия
Направленность (профиль) Цифровые технологии и интеллектуальные инженерные решения

Присваиваемая квалификация
"Магистр"

Формы обучения
очная

1 Паспорт комплекта оценочных материалов

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
тестирование, подготовка отчетов по практическим и (или) лабораторным работам	ОПК-7	Применяет при решении профессиональных задач методы и средства получения, хранения, переработки и трансляции информации посредством современных компьютерных технологий, в том числе, в глобальных компьютерных сетях	Знать базовые понятия информационной безопасности, принципы и подходы к защите информации при работе с современными компьютерными технологиями и глобальными сетями, нормативно-правовые и стандартизированные требования к защите данных. Уметь анализировать задачи по защите информации и формировать требования к обеспечению безопасности на основе оценки рисков Владеть практическими навыками использования современных инструментов.	Высокий или средний
тестирование, подготовка отчетов по практическим и (или) лабораторным работам	ПК-4	Владеет знаниями нормативно правовых актов, методических документов, национальных стандартов в области защиты интеллектуальной собственности.	Владеет знаниями нормативно правовых актов, методических документов, национальных стандартов в области защиты интеллектуальной собственности. Уметь использовать нормативные и правовые акты в профессиональной деятельности. Владеть навыками установки и настройки программных (программно-технических) средств защиты информации от несанкционированного доступа.	Высокий или средний
Высокий уровень достижения компетенции - компетенция сформирована частично, рекомендованные оценки: отлично, хорошо, зачтено. Средний уровень достижения компетенции - компетенция сформирована частично, рекомендованные оценки: хорошо, удовлетворительно, зачтено. Низкий уровень достижения компетенции - компетенция не сформирована частично, оценивается неудовлетворительно или не зачтено.				

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.

2.1.Оценочные материалы при текущем контроле

Текущий контроль по темам дисциплины заключается в тестирование, подготовка отчетов по практическим и(или) лабораторным работам.

Тестирование

При проведении тестирования обучающимся необходимо ответить на 20 тестовых вопросов. За каждый правильно данный ответ обучающийся получает 5 баллов.

Шкала оценивания:

Количество баллов	0-64	65-74	75-84	85-100
Шкала оценивания	Неуд	Удовлетворительно	Хорошо	Отлично
	Не зачтено	Зачтено		

Пример тестовых заданий:

ОПК-7 - Способен применять при решении профессиональных задач методы и средства получения, хранения, переработки и трансляции информации посредством современных компьютерных технологий, в том числе, в глобальных компьютерных сетях

Содержание вопроса (задания)	Правильный ответ
Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению _____ такой информации.	Конфиденциальности
Техническая защита информации - это защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и _____ средств.	программно-технических

ПК-4 - Способность проводить патентные исследования, владеть методами и средствами защиты интеллектуальной собственности

Содержание вопроса (задания)	Правильный ответ
В государственных органах, органах местного самоуправления документирование информации осуществляется в соответствии с _____, установленными уполномоченным федеральным органом исполнительной власти в сфере архивного дела и делопроизводства.	правилами делопроизводства
Физическая защита информации - это защита информации путем _____ мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.	организационных

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 материалы при промежуточной аттестации

Формами промежуточной аттестации являются экзамен, 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 экзамене обучающийся отвечает на 2 вопроса или проходит тестирование.

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	
	Не зачтено		Зачтено		

Примерный перечень вопросов на экзамен:

1. В чем заключается биометрическая аутентификация пользователей, какие у нее достоинства и недостатки.
2. В чем заключается их основное назначение?
3. В чем заключается процедура простой аутентификации, какими способами она производится, поясните схематично ее реализацию с использованием пароля.
4. Виды тайн, охраняемых в соответствии с федеральным законодательством.
5. Государственная тайна в системе информационной безопасности РФ. Общая характеристика правовых основ защиты государственной тайны.
6. Для чего она нужна?
7. Европейская Конвенция о защите прав человека и основных свобод.
8. Защита государственной тайны. Органы защиты государственной тайны.
9. Интересы государства в информационной сфере.
10. Интересы личности в информационной сфере.
11. Интересы общества в информационной сфере.
12. Как можно классифицировать модели угроз?
13. Как она помогает в обеспечении защиты?
14. Как угрозы связаны с нарушением принципов конфиденциальности, целостности и доступности?
15. Какие основные этапы включает построение модели угроз?
16. Какие существуют виды угроз безопасности информации? Приведите примеры.
17. Каким образом модель угроз может быть использована в рамках системы защиты информации?
18. Какими способами блокируется угроза несанкционированного копирования информации ПЭВМ, в чем они заключаются, раскройте их содержание.
19. Классификация угроз информационной безопасности РФ.
20. Классифицируйте угрозы по типу (например, вирусы, социальная инженерия, физические атаки).
21. Конвенция Совета Европы "О защите личности в связи с автоматизированной обработкой персональных данных".
22. Конфиденциальная информация. Понятие, особенности правового закрепления, виды.
23. Кто должен разрабатывать модели угроз? (Самостоятельно или с помощью третьих лиц)
24. Массовая информация как объект регулирования. Основные принципы распространения массовой информации.
25. Международное информационное законодательство.
26. Международные нормативно-правовые акты о неприкосновенности честной жизни лица, личной и семейной тайне.
27. Модельный закон Межпарламентской Ассамблеи Содружества государств "О защите персональных данных".
28. Назовите и опишите основные модели разграничения доступа (дискреционное, мандатное,

ролевое).

29. Неприкосновенность частной жизни. Личная и семейная тайна.

30. Основные направления обеспечения информационной безопасности в области внешней и внутренней политики РФ.

31. Основные положения государственной политики обеспечения информационной безопасности РФ.

32. Основные функции системы обеспечения информационной безопасности РФ.

33. Основные элементы организационной основы системы обеспечения информационной безопасности РФ

34. Особенности и основные направления международного сотрудничества в области обеспечения информационной безопасности РФ.

35. Перечень сведений, составляющих государственную тайну.

36. Перечислите базовые технологии (механизмы) безопасности информации в компьютерных системах. Дайте определение процессам идентификации, аутентификации и авторизации для обеспечения защиты информации. Дайте определение понятиям: пароль; персональный идентификационный номер; динамический пароль; система запрос-пароль; сертификаты и цифровые подписи.

37. Перечислите защитные механизмы, реализуемые программно-аппаратными комплексами (средствами) защиты информации в компьютерных системах (ПЭВМ). Дайте определение понятию - «субъект доступа», какие процедуры реализуются при его обращении к компьютерной системе.

38. Перечислите методы ограничения доступа к компонентам ЭВМ, какие применяют средства для ограничения доступа к компонентам ЭВМ.

39. Персональные данные как особый институт охраны прав на неприкосновенность частной жизни.

40. Полномочия органов государственной власти и должностных лиц в области отнесения сведений к государственной тайне и их защиты.

41. Понятие и виды угроз информационной безопасности РФ.

42. Понятие и классификация общих методов обеспечения информационной безопасности РФ.

43. Понятие и система правовых основ информационной безопасности.

44. Понятие информационной безопасности РФ.

45. Понятие национальных интересов РФ в информационной сфере и их обеспечение.

46. Понятие персональных данных и проблемы их правовой регламентации.

47. Понятие, признаки, виды и общая характеристика преступлений в информационной сфере.

48. Почему компьютерные вирусы причисляют к особому классу разрушающих программных воздействий. Раскройте классификацию и жизненный цикл компьютерных вирусов.

49. Почему компьютерные вирусы причисляют к особому классу разрушающих программных воздействий. Раскройте основные каналы распространения компьютерных вирусов и других вредоносных программ.

50. Почему компьютерные вирусы причисляют к особому классу разрушающих программных воздействий. Перечислите и дайте определение методам обнаружения компьютерных вирусов и видам антивирусных программ. Критерии качества антивирусной программы.

51. Правовая охрана и защита прав на неприкосновенность частной жизни.

52. Правовые проблемы информационной безопасности. Механизмы защиты

53. Признаки, состав и характеристика правонарушений в информационной сфере.

54. Принципы государственной политики обеспечения информационной безопасности РФ.

55. Раскройте основные методы аутентификации, использующие пароли и PIN-коды. Поясните на структурных схемах простую аутентификацию пользователя ресурсов компьютерной системы с использованием пароля и аутентификацию, основанную на использовании односторонней хэшфункции для проверки пароля.

56. Российская правовая регламентация неприкосновенности частной Декларация о правах и свободах человека и гражданина Российской Федерации

57. Секретность информации как правовая категория. Уровни доступа регулирование.

58. Соотношение информационного законодательства и законодательства об интеллектуальной собственности.

59. Состояние информационной безопасности РФ и основные задачи по ее обеспечению

60. Тенденции и основные проблемы развития информационного права.

61. Уголовное законодательство в области защиты информации.

62. Уголовно-правовая защита государственной тайны в РФ.

63. Что такое «базовая модель угроз» ФСТЭК?

64. Что такое модель безопасности?

65. Что такое модель угроз информационной безопасности?

Критерии оценивания при тестировании:

- 95-100 баллов – при правильном и полном ответе на 19-20 вопросов;
- 85...94 баллов – при правильном ответе на 16-18 вопросов;
- 75...84 баллов – при правильном ответе на 13-15 вопросов;
- 65...74 баллов – при правильном ответе на 10-12 вопросов
- 25...64 – при правильном ответе только на 1-9 вопрос(ов);
- 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	
	Не зачтено		Зачтено		

Примерный перечень тестовых вопросов на экзамен:

ОПК-7 - Способен применять при решении профессиональных задач методы и средства получения, хранения, переработки и трансляции информации посредством современных компьютерных технологий, в том числе, в глобальных компьютерных сетях

Содержание вопроса (задания)		Правильный ответ
В ходе верификации ____ ? Выберите все верные 1. выявляются несоответствия поведения системы требованиям 2. устраняются ошибки и дефекты программной системы 3. регистрируются выявленные дефекты и проблемы 4. составляются отчеты об устраненных проблемах		1, 2, 4
Какие инструменты чаще всего используются при проведении анализа защищенности программного обеспечения? 1. Антивирусные программы 2. Средства мониторинга сетевого трафика 3. Программы для создания бэкапов		2
Установите соответствие между методом (левый столбец) и его сущностью (правый столбец).		А-2, Б-1, В-3.
Метод	Сущность	
А. Симметричное шифрование	1. Использует пару ключей: открытый для шифрования и закрытый для расшифрования	
Б. Асимметричное шифрование	2. Использует один секретный ключ для шифрования и расшифрования	
В. Хеширование	3. Преобразует данные в строку фиксированной длины, необратимую для восстановления	
Установите соответствие между типом угрозы (левый столбец) и её описанием (правый столбец)		А-2, Б-1, В-3.
Угроза	Описание	
А. DDoS-атака	1. Перехват и возможное изменение данных между устройствами	
Б. Человек посередине (MITM)	2. Массовые запросы, перегружающие сервер или сеть	
В. Вредоносное ПО	3. Программы, нарушающие работу системы или крадущие данные	
Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению такой информации.		Конфиденциальности
Техническая защита информации - это защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и _____ средств.		программно-технических

Какие требования содержит модель системы безопасности с полным перекрытием?	требования к составу подсистемы защиты
Первая модель при разработке системы безопасности это	модель объекта
_____ тайна - режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.	Коммерческая
_____ имя - обозначение символами, предназначенное для адресации сайтов в сети «Интернет» в целях обеспечения доступа к информации, размещенной в сети «Интернет»	Доменное

ПК-4 - Способность проводить патентные исследования, владеть методами и средствами защиты интеллектуальной собственности

Содержание вопроса (задания)	Правильный ответ
В государственных органах, органах местного самоуправления документирование информации осуществляется в соответствии с _____, установленными уполномоченным федеральным органом исполнительной власти в сфере архивного дела и делопроизводства.	правилами делопроизводства
Физическая защита информации - это защита информации путем _____ мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.	организационных
Цели информационной безопасности - своевременное обнаружение, предупреждение _____, воздействия в сети.	несанкционированного доступа
Информация, переданная или полученная пользователем информационно-телекоммуникационной сети.	электронное сообщение
Кто назначается ответственным за определение уровня классификации информации.	владелец
Укажите категорию, которая является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности.	сотрудники

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.