

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: 05.05.2026 Н24:34:01

Д.М. Дубинкин

Фонд оценочных средств дисциплины

Управление информационной безопасностью

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

Присваиваемая квалификация
"Магистр"

Формы обучения
очно-заочная

5.1 Паспорт комплекта оценочных материалов

Планируемые результаты обучения по дисциплине (модулю)

Дисциплина направлена на формирование следующих компетенций выпускника:

Ф о р м а (ы) т е к у щ е г о к о н т р о л я	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	ОПК-1	Обосновывает требования к системе обеспечения информационной безопасности и разрабатывает проекты технического задания на ее создание	Знать основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; основные механизмы информационной безопасности и типовые процессы управления этими механизмами в информационной системе; основные угрозы безопасности информации и модели нарушителя в информационных системах; принципы формирования политики информационной безопасности в информационных системах; методы аттестации уровня защищенности информационных систем; основные методы управления информационной безопасностью; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем. Уметь строить системы обеспечения информационной безопасности в различных условиях функционирования защищаемых информационных систем; разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; разрабатывать частные политики информационной безопасности информационных систем; контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем; оценивать информационные риски в информационных системах; разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем; составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности. Владеть методами и средствами выявления угроз безопасности информационным системам; навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем; навыками участия в экспертизе состояния защищенности информации на объекте защиты; методами управления информационной безопасностью информационных систем; методами оценки информационных рисков; методами организации и управления деятельностью служб защиты информации на предприятии; навыками управления информационной безопасностью простых объектов.	Высокий или средний
--	-------	---	--	---------------------

Опрос по контрольным вопросам, подготовка отчетов по практическим и (или) лабораторным работам	ОПК-3	Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	Знает нормативную и правовую базу в области управления информационной безопасностью объектов критической информационной инфраструктуры. Знает отечественные и зарубежные стандарты в области управления информационной безопасностью объектов критической информационной инфраструктуры. Знает структуру политик обеспечения информационной безопасности объектов критической информационной инфраструктуры и требования к их содержанию. Умеет разрабатывать проекты нормативных и организационно-распорядительных документов по обеспечению информационной безопасности объектов критической информационной инфраструктуры. Умеет разрабатывать политику информационной безопасности объектов критической информационной инфраструктуры различных уровней. Владеет навыками разработки политики информационной безопасности различных уровней	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.				

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 материалы при текущем контроле

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

Опросе обучающихся по контрольным вопросам

Обучающийся отвечает на 2 вопроса.

Например:

ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;

Содержание вопроса (задания)	Правильный ответ
Основной процесс управления ИБ, результатом которого является перечень недопустимых последствий и обоснование необходимости внедрения конкретных мер защиты в ТЗ, называется оценка _____.	рисков
Высокоуровневый документ организации, на основе которого формулируются общие требования к проектируемой системе защиты и определяются цели обеспечения безопасности, называется _____ информационной безопасности.	политика

ОПК-3 Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;

Содержание вопроса (задания)	Правильный ответ
Совокупность документов, регламентирующих вопросы защиты информации и изданных руководством организации в рамках своей компетенции, составляет организационно-_____ документацию по ИБ.	распорядительную
При разработке проекта документа, устанавливающего запрет на разглашение коммерческой тайны, обязательным приложением к трудовому договору является _____ о неразглашении.	Обязательство

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

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.

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		
Шкала оценивания	Не зачтено	Зачтено			

Примерный перечень вопросов на экзамен:

ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;

Содержание вопроса (задания)	Правильный ответ
Основной процесс управления ИБ, результатом которого является перечень недопустимых последствий и обоснование необходимости внедрения конкретных мер защиты в ТЗ, называется оценка _____.	рисков

Содержание вопроса (задания)	Правильный ответ
Высокоуровневый документ организации, на основе которого формулируются общие требования к проектируемой системе защиты и определяются цели обеспечения безопасности, называется _____ информационной безопасности.	политика

ОПК-3 Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;

Содержание вопроса (задания)	Правильный ответ
Совокупность документов, регламентирующих вопросы защиты информации и изданных руководством организации в рамках своей компетенции, составляет организационно-_____ документацию по ИБ.	распорядительную
При разработке проекта документа, устанавливающего запрет на разглашение коммерческой тайны, обязательным приложением к трудовому договору является _____ о неразглашении.	Обязательство
Реквизит документа, содержащий дату, регистрационный номер и место составления, называется _____ данными документа.	справочными
Документ, определяющий задачи, функции, права и ответственность подразделения (отдела), отвечающего за защиту информации в компании, называется _____ об отделе ИБ.	Положение

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	85-94	95-100
Шкала оценивания	Неуд	Удовлетворительно	Хорошо	Отлично	
	не зачтено	зачтено			

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;

Содержание вопроса (задания)	Правильный ответ
Какой процесс в управлении ИБ является первичным для обоснования выбора мер защиты и формирования требований в техническом задании? 1. Закупка оборудования. 2. Оценка рисков информационной безопасности. 3. Написание должностных инструкций. 4. Проведение инвентаризации мебели в офисе.	2
При разработке ТЗ требование к «минимизации прав доступа», когда пользователю предоставляются только те полномочия, которые необходимы для выполнения работы, обосновывается принципом: 1. Максимальной открытости. 2. Производственной необходимости (наименьших привилегий). 3. Удобства администрирования. 4. Экономии оперативной памяти.	2
Установите соответствие методов обработки рисков и проектных решений в ТЗ	А - 2, Б - 3, В - 1.
Метод обработки риска	
А) Снижение (минимизация)	
Б) Передача (перекладывание)	
В) Уклонение (избегание)	
Техническое/организационное решение в ТЗ	
1) Отказ от использования облачных сервисов для хранения гостайны	
2) Внедрение системы двухфакторной аутентификации и шифрования	
3) Заключение договора страхования киберрисков или аутсорсинг ИБ	

Содержание вопроса (задания)		Правильный ответ
Установите соответствие документов по управлению ИБ и их роли при разработке ТЗ		А - 2, Б - 1, В - 3.
Документ	Роль в обосновании требований	
А) Политика ИБ	1) Описание конкретных векторов атак для выбора средств защиты	
Б) Модель угроз	2) Фундамент, определяющие общие принципы и цели защиты	
В) Техническое задание	3) Детальный перечень требований к реализации системы защиты	
Установите правильную последовательность этапов управления рисками для обоснования требований к системе защиты: 1. Выбор мер и средств защиты для нейтрализации угроз. 2. Идентификация информационных активов и их ценности. 3. Анализ и оценка вероятности реализации угроз. 4. Определение остаточного риска после внедрения мер.		2, 3, 1, 4.
Расставьте уровни нормативного обоснования требований к системе ИБ в порядке убывания их приоритетности (от общегосударственных к локальным): 1. Корпоративные инструкции и регламенты организации. 2. Федеральные законы и указы Президента РФ. 3. Отраслевые стандарты и требования регуляторов (ФСТЭК/ФСБ). 4. Политика информационной безопасности предприятия.		2, 3, 4, 1.

ОПК-3 Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;

Содержание вопроса (задания)		Правильный ответ
Какой локальный нормативный акт является документом верхнего уровня в системе управления ИБ и служит базой для разработки всех остальных организационно-распорядительных документов? 1. 1. Инструкция по антивирусной защите. 2. 2. Политика информационной безопасности. 3. 3. Журнал учета машинных носителей. 4. 4. Приказ о назначении системного администратора.		2
Каким распорядительным документом в организации официально вводится в действие проект разработанного «Положения о защите персональных данных»? 1. 1. Служебной запиской. 2. 2. Приказом руководителя. 3. 3. Протоколом совещания. 4. 4. Трудовым договором.		2
Установите соответствие распорядительных документов и их целей в управлении ИБ		А - 2, Б - 3, В - 1.
Вид документа	Цель разработки документа	
А) Приказ	1) Описание детального порядка действий при инцидентах	
Б) Положение	2) Назначение ответственных лиц и ввод документов в действие	
В) Регламент	3) Определение структуры и функций подразделения защиты	
Установите соответствие реквизитов документа ИБ и их назначения (по ГОСТ)		А - 2, Б - 1, В - 3.
Реквизит	Значение для управления документом	
А) Гриф утверждения	1) Подтверждение согласия должностного лица с проектом	
Б) Виза согласования	2) Придание документу официальной юридической силы	
В) Гриф секретности	3) Определение правил обращения с носителем информации	

Содержание вопроса (задания)	Правильный ответ
Расположите типы документов по информационной безопасности в порядке убывания их приоритетности в иерархии системы управления ИБ (СУИБ): 1. 1. Регламент проведения антивирусных проверок. 2. 2. Федеральное законодательство в области ИБ. 3. 3. Политика информационной безопасности организации. 4. 4. Должностная инструкция администратора ИБ.	2, 3, 1, 4.
Установите последовательность действий при подготовке проекта приказа о назначении ответственных за защиту персональных данных: 1. 1. Визирование проекта приказа у юриста и начальника отдела кадров. 2. 2. Определение круга должностных лиц, которые будут обрабатывать данные. 3. 3. Регистрация подписанного приказа и присвоение ему номера. 4. 4. Составление текста приказа с указанием конкретных обязанностей лиц.	2, 4, 1, 3.

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.