

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 Н24:32:43

Д.М. Дубинкин

Фонд оценочных средств дисциплины

Построение моделей угроз 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 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
Опрос по контрольным вопросам, подготовка отчетов по практическим и (или) лабораторным работам	ПК-6	Способен построить модель угроз информационной безопасности, выявлять и оценивать актуальности угроз информационной безопасности, построения их моделей для определения требований о защите информации.	Знает общую информацию об угрозах и нарушителях безопасности информации компьютерных систем. Знает методику выявления и оценки актуальности угроз информационной безопасности, построения их моделей для определения требований о защите информации. Умеет выявлять и оценивать актуальности угроз информационной безопасности, построения их моделей для определения требований о защите информации. Владеет навыками работы с нормативными документами по определению требований о защите информации компьютерных систем.	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 в оформлении отчетов по лабораторным работам.

Опросе обучающихся по контрольным вопросам

Обучающийся отвечает на 2 вопроса.

Например:

Содержание вопроса (задания)	Правильный ответ
_____ - это нарушители, не имеющие прав доступа в контролируруемую (охраняемую) зону (территорию) и (или) полномочий по доступу к информационным ресурсам и компонентам систем и сетей, требующим авторизации	внешние нарушители
_____ - это потенциальная возможность определенным образом нарушить информационную безопасность	угроза

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 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		
Шкала оценивания	Не зачтено	Зачтено			

Примерный перечень вопросов на экзамен:

Содержание вопроса (задания)	Правильный ответ
___ - это нарушители, не имеющие прав доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочий по доступу к информационным ресурсам и компонентам систем и сетей, требующим авторизации	внешние нарушители
___ - это потенциальная возможность определенным образом нарушить информационную безопасность	угроза
___ - это попытка реализации угрозы	атака
___ - это состояние, в котором находится объект безопасности вследствие возникновения угрозы этому объекту	опасность

___ - это промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется	окно опасности
Показатель, определяемый как произведение вероятности реализации угрозы и величины возможного ущерба для организации, называется _____ информационной безопасности.	риском
Недостаток или слабое место в системе защиты, программном обеспечении или аппаратных средствах, которое может быть использовано нарушителем для реализации угрозы, называется _____.	уязвимостью
Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации, называется _____ информационной безопасности.	угрозой

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

ПК-6 Прогнозирует риски в информационной безопасности и управляет инцидентами информационной безопасности

Содержание вопроса (задания)	Правильный ответ
Что НЕ относится к категориям угроз: 1. по масштабу; 2. по характеру ущерба; 3. расположение источника; 4. по скорости возникновения.	4
Укажите адрес информационного сайта на котором размещены общий перечень угроз безопасности информации, содержащейся в банке данных угроз безопасности информации ФСТЭК России: 1. fsb.ru 2. bdu.fstec.ru 3. бду.фстэк.пф 4. cert.gov.ru/o-nktski	2
Какой этап не входит в оценку угроз безопасности информации? 1. определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации; 2. определение возможных объектов воздействия угроз безопасности информации; 3. оценку возможности реализации (возникновения) угроз безопасности информации и определение их актуальности; 4. определение лиц информационного взаимодействия.	4
По результатам определения источников угроз безопасности информации должны быть определены (множественный выбор): 1. виды актуальных нарушителей и возможные цели реализации ими угроз безопасности информации, а также их возможности; 2. список программного обеспечения; 3. категории актуальных нарушителей, которые могут реализовать угрозы безопасности информации; 4. страну происхождения программных продуктов и программных комплексов.	1, 3

Содержание вопроса (задания)		Правильный ответ
Сопоставьте название нормативно-правовых актов с их реквизитами		А-4, Б-3, В-2, Г-1
А. №149-ФЗ от 27.07.2006 г.	1. Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений	
Б. №187-ФЗ от 26.07.2017 г.	2. О персональных данных	
В. №152-ФЗ от 27.07.2006 г.	3. О безопасности критической информационной инфраструктуры Российской Федерации	
Г. №117 от 11.04.2025 г.	4. Об информации, информационных технологиях и о защите информации	
Установите соответствие стратегий управления рисками и защитных мер		А - 2, Б - 1, В - 3.
Стратегия	Пример реализации в модели	
А) Снижение риска	1) Отказ от использования беспроводных сетей в организации	
Б) Избегание риска	2) Установка системы обнаружения вторжений (IDS)	
В) Передача риска	3) Страхование ответственности за утечку данных	
Установите соответствие методов оценки и их специфики		А - 2, Б - 1, В - 3.
Метод оценки риска	Специфика подхода	
А) Качественный	1) Расчет ущерба в денежном эквиваленте (рубли, доллары)	
Б) Количественный	2) Оценка по шкале «высокий / средний / низкий»	
В) Комбинированный	3) Использование балльных оценок вместе с финансовым прогнозом	
Установите соответствие видов последствий и нарушаемых свойств информации		А - 2, Б - 3, В - 1.
Тип последствия	Нарушаемое свойство	
А) Опубликование персональных данных в сети	1) Целостность	
Б) Удаление базы данных без возможности восстановления	2) Конфиденциальность	
В) Подмена суммы транзакции в банковской системе	3) Доступность	
Установите соответствие уровней актуальности угроз (по методике ФСТЭК) и их описания		А - 2, Б - 1, В - 3.
Уровень актуальности	Описание	
А) Актуальная угроза	1) Малая вероятность реализации и низкая степень ущерба	
Б) Неактуальная угроза	2) Высокая вероятность реализации или значительный ущерб	
В) Потенциальная угроза	3) Теоретически возможная угроза без привязки к конкретной системе	

Содержание вопроса (задания)		Правильный ответ
Установите соответствие компонентов риска и их определений		А - 2, Б - 1, В - 3.
Компонент	Определение	
А) Угроза	1) Слабое место в защите или ошибка в программном коде	
Б) Уязвимость	2) Потенциальная возможность нарушения безопасности информации	
В) Ущерб	3) Негативные последствия реализации угроз (финансовые, репутационные)	
Установите последовательность действий при анализе модели нарушителя: 1. 1. Определение категории нарушителя (внутренний/внешний). 2. 2. Оценка потенциала и ресурсов нарушителя (низкий, средний, высокий). 3. 3. Описание вероятных целей нарушителя. 4. 4. Определение доступных нарушителю точек входа в систему.		1, 3, 2, 4.
Расставьте шаги оценки рисков ИБ в логической последовательности: 1. 1. Идентификация ценных активов и их уязвимостей. 2. 2. Расчет вероятности реализации угроз. 3. 3. Определение величины потенциального ущерба. 4. 4. Сравнение расчетного уровня риска с допустимым порогом.		1, 3, 2, 4.
Установите порядок действий нарушителя при реализации атаки в модели: 1. 1. Эксплуатация выявленной уязвимости. 2. 2. Разведка и поиск слабых мест в защите. 3. 3. Достижение конечной цели (хищение или порча данных). 4. 4. Закрепление в системе и повышение привилегий.		2, 1, 4, 3.
Установите последовательность действий при управлении рисками после их оценки: 1. 1. Выбор стратегии обработки (снижение, перенос, принятие, избегание). 2. 2. Разработка плана внедрения дополнительных мер защиты. 3. 3. Оценка остаточного уровня риска. 4. 4. Утверждение итоговой модели руководством.		1, 2, 3, 4.
Расположите действия эксперта для определения актуальности угрозы: 1. 1. Определение частоты возникновения угрозы в аналогичных системах. 2. 2. Оценка технической возможности реализации угрозы в текущей архитектуре. 3. 3. Определение уровня ущерба для бизнес-процессов. 4. 4. Принятие решения об актуальности (актуальна / не актуальна).		2, 1, 3, 4.
Установите последовательность действий при переходе от прогнозирования к реагированию: 1. 1. Разработка сценариев реагирования на прогнозируемые угрозы. 2. 2. Включение сценариев в инструкции персонала по управлению инцидентами. 3. 3. Определение признаков (индикаторов) срабатывания угрозы в модели. 4. 4. Мониторинг событий безопасности на основе модели.		3, 1, 2, 4.

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.