МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Филиал КузГТУ в г. Новокузнецке

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 71B13ADF852F0D849D78875814FBEF47
Владелец: Баранов Юрий Александрович
Действителен: с 15.10.2025 до 08.01.2027

УТВЕРЖДЕНО

Заместитель директора,
совмещающий обязанности директора
филиала КузГТУ в г. Новокузнецке

_____Баранов Ю.А.

«29» мая 2026г.

Рабочая программа дисциплины

Построение моделей угроз информационной безопасности

Направление подготовки 10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль) Анализ безопасности информационных систем

Присваиваемая квалификация «Специалист по защите информации»

Формы обучения: очная

Год набора 2026

Новокузнецк 2026 г.

Рабочая программа обсуждена на заседании учебно-методического совета филиала КузГТУ в г. Новокузнецке

Протокол № 6 от 29.05.2026

Зав. Кафедрой ИТиЭД _____ В. В. Шарлай
подпись

СОГЛАСОВАНО:

Заместитель директора по УР _____ Т. А. Евсина
подпись

1 Перечень планируемых результатов обучения по дисциплине "Построение моделей угроз информационной безопасности", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:

общепрофессиональных компетенций:

ОПК-2 - Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности;

Результаты обучения по дисциплине определяются индикаторами достижения компетенций

Индикатор(ы) достижения:

Способен построить моделей угроз информационной безопасности с использованием программных средств прикладного назначения, выявлять и оценивать актуальности угроз информационной безопасности, построения их моделей для определения требований о защите информации

Результаты обучения по дисциплине:

Знает общую информацию об угрозах и нарушителях безопасности информации компьютерных систем. Знает программные средств прикладного назначения, в том числе отечественного производства для построения моделей угроз. 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.

2 Место дисциплины "Построение моделей угроз информационной безопасности" в структуре ОПОП специалитета

Для освоения дисциплины необходимы знания умения, навыки и (или) опыт профессиональной деятельности, полученные в рамках изучения следующих дисциплин: Проектный практикум, Безопасность систем баз данных, Организационное и правовое обеспечение информационной безопасности, Основы информационной безопасности, Практикум по виду профессиональной деятельности, Нормативные требования по защите информации, Информационные угрозы, Технические средства охраны объектов информатизации, Безопасность программного обеспечения, Безопасность сетей электронных вычислительных машин.

Дисциплина входит в Блок 1 «Дисциплины (модули)» ОПОП. Цель дисциплины - получение обучающимися знаний, умений, навыков и (или) опыта профессиональной деятельности, необходимых для формирования компетенций, указанных в пункте 1.

3 Объем дисциплины "Построение моделей угроз информационной безопасности" в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины "Построение моделей угроз информационной безопасности" составляет 5 зачетных единиц, 180 часов.

Форма обучения	Количество часов		
	ОФ	ЗФ	ОЗФ
Курс 5/Семестр 10			
Всего часов	180		
Контактная работа обучающихся с преподавателем (по видам учебных занятий):			
Аудиторная работа			
Лекции	32		
Лабораторные занятия			

Форма обучения	Количество часов		
	ОФ	ЗФ	ОЗФ
Практические занятия	48		
Внеаудиторная работа			
Индивидуальная работа с преподавателем:			
Курсовая работа	2		
Консультация и иные виды учебной деятельности			
Самостоятельная работа под руководством преподавателя	52		
Самостоятельная работа	46		
Форма промежуточной аттестации	зачет		

4 Содержание дисциплины "Построение моделей угроз информационной безопасности", структурированное по разделам (темам)

4.1. Лекционные занятия

Раздел дисциплины, темы лекций и их содержание	Трудоемкость в часах
	ОФ
1.Модели нарушителей информационной безопасности Возможности нарушителей (модель нарушителя); Типы и виды нарушителей; Возможные цели и потенциал нарушителей; Типовые модели нарушителей; Классификация угроз информационной безопасности объектов информатизации	10
2. Угрозы информационной безопасности и уязвимости объектов информатизации Угрозы и уязвимости; Возможные способы реализации угроз безопасности информации; Актуальные угрозы безопасности информации; Типовые модели угроз информационной безопасности;	10
3. Анализ рисков реализации угроз информационной безопасности Разработка модели угроз; Способы оценки рисков реализации угроз информационной безопасности; Методические рекомендации по оценке рисков реализации угроз информационной безопасности; Методика определения угроз безопасности информации в информационных системах;	12
Итого	**32**

4.2. Практические (семинарские) занятия

Тема занятия	Трудоемкость в часах
	ОФ
1. Типовые модели нарушителей ИБ ОИ на базе компьютерных систем	16
2. Типовые модели угроз информационной безопасности Уязвимости объектов информатизации	16
3. Анализ актуальности реализации угроз информационной безопасности	16
Итого	**48**

4.3 Самостоятельная работа обучающегося и перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Вид СРС	Трудоемкость в часах
	ОФ
Ознакомление с содержанием основной и дополнительной литературы, методических материалов, конспектов для подготовки к занятиям	14
Оформление отчетов по практическим и(или) лабораторным работам	16
Подготовка курсоой работы/проекта	10
Подготовка к промежуточной аттестации	6
Итого	46
Самостоятельная работа под руководством преподавателя, в т.ч. подготовка курсоой работы/проекта	52

Самостоятельная работа под руководством преподавателя:

Внеаудиторная самостоятельная работа выполняется обучающимся самостоятельно по индивидуальным заданиям, полученным от педагогического работника, но без его непосредственного участия.

В ходе выполнения самостоятельной работы педагогический работник осуществляет непосредственное руководство процессом выполнения индивидуальной самостоятельной работы в форме текущего контроля успеваемости. Текущий контроль успеваемости обеспечивает оценивание хода самостоятельного освоения дисциплины (практик). Для организации самостоятельной работы обучающегося по индивидуальным заданиям, полученным от педагогического работника, а так же показатели и критерии оценивания, описание шкал оценивания результатов самостоятельной работы, используются оценочные материалы, размещенные в фондах оценочных средств для текущего контроля успеваемости обучающихся.

4.4 Курсовое проектирование (курсовая работа)

Курсовая работа/проект является формой промежуточной аттестации обучающихся по дисциплине, контактная работа с преподавателем - 2 часа.

5 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине "Построение моделей угроз информационной безопасности"

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	ОПК-2	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 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. Последствия инцидентов ИБ.
2. Цели управления инцидентами 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:

1. Методика определения угроз безопасности информации в информационных системах
2. Способы оценки рисков реализации угроз информационной безопасности

3. Порядок разработки модели угроз

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 являютя зачет, курсовая работа, 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;

Курсовая работа/проект является формой промежуточной аттестации обучающихся по дисциплине.

Курсовая работа/проект выполняется обучающимися с целью:

формирования навыков применения теоретических знаний, полученных в ходе освоения дисциплины;
формирования практических навыков в части сбора, анализа и интерпретации результатов, необходимых для последующего выполнения научных научно-исследовательской работы;
формирования навыков логически и последовательно иллюстрировать подготовленную в процессе выполнения курсовой работы/проекта информацию;
формирования способностей устанавливать закономерности и тенденции развития явлений и процессов , анализировать , обобщать и формулировать выводы;
формировать умение использовать результаты, полученные в ход е выполнения курсовой работы/проекта в профессиональной деятельности.

Тема курсовой работы/проекта выбирается обучающимся самостоятельно.

Примерные темы курсовых работ/проектов:

1. Сравнительный анализ методик моделирования угроз
2. Автоматизация процесса построения моделей угроз с использованием специализированного ПО
3. Разработка алгоритма классификации нарушителей информационной безопасности для конкретной отрасли
4. Построение модели угроз для облачных инфраструктур
5. Анализ угроз и моделирование векторов атак на системы «умного дома»
6. Специфика моделирования угроз для критических информационных систем (КИИ) в энергетической сфере.
7. Модель угроз безопасности для мобильных приложений банковского сектора.
8. Угрозы безопасности при использовании технологий искусственного интеллекта и машинного обучения в корпоративных сетях.
9. Разработка модели угроз для образовательного учреждения с учетом дистанционных технологий обучения.
10. Особенности моделирования угроз для малого бизнеса в условиях ограниченного бюджета на ИБ.
11. Модель угроз для государственных информационных систем (ГИС) в соответствии с актуальными требованиями регуляторов.

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 зачет:

1. Правовое регулирование отношений по защите информации в информационных и телекоммуникационных сетях, а также в сети Интернет.
2. Классификация объектов информатизации.
3. Правовой порядок установления соответствия параметров объектов информатизации и средств защиты информации требованиям нормативных документов.

Пример тестовых вопросов:

1. В настоящее время наиболее широко распространены системы управления базами данных

а) иерархические

+ б) реляционные

в) сетевые

г) объектно-ориентированные

2. СУБД Oracle, Informix, Subase, DB 2, MS SQL Server относятся к

а) сетевым

б) иерархическим

+ г) реляционным

д) объектно-ориентированным

3. Традиционным методом организации информационных систем является

+ а) архитектура клиент-сервер

б) архитектура клиент-клиент

в) архитектура сервер-сервер

г) размещение всей информации на одном компьютере

4. Жизненный цикл ИС регламентирует стандарт ISO/IEC 12207. IEC – это

а) международная организация по стандартизации

+ б) международная комиссия по электротехнике

в) международная организация по информационным системам

г) международная организация по программному обеспечению

5. Согласно ISO 12207, объединение одного или нескольких процессов, аппаратных средств, программного обеспечения, оборудования и людей для удовлетворения определённым потребностям или целям это

а) полнофункциональный программно-аппаратный комплекс

б) информационная система

+ в) система

г) вычислительный центр

6. Какое определение информационных ресурсов общества соответствует Федеральному закону " Об информации, информатизации и защите информации"

+ а) Информационные ресурсы общества – это отдельные документы и отдельные массивы документов, документы и массивы в информационных системах (библиотеках, архивах, фондах, банках данных и других системах), созданные, приобретенные за счет средств федерального бюджета, бюджетов субъектов РФ.

б) Информационные ресурсы общества – это сведения различного характера, материализованные в виде документов, баз данных и баз знаний.

в) Информационные ресурсы общества – это множество web-сайтов, доступных в Интернете.

7. Какой информационной системе соответствует следующее определение: программно-аппаратный комплекс, способный объединять в одно целое предприятия с различной функциональной

направленностью (производственные, торговые, кредитные и др. организации)

а) Информационная система промышленного предприятия.

б) Информационная система торгового предприятия.

+ в) Корпоративная информационная система.

г) Информационная система кредитного учреждения.

8. Открытая информационная система это

+ а) Система, созданная на основе международных стандартов.

б) Система, включающая в себя большое количество программных продуктов.

в) Система, ориентированная на оперативную обработку данных.

г) Система, включающая в себя различные информационные сети.

9. Информационные модели предназначены для

+ а) отражения информационных потоков между объектами и
отношений между ними

б) математического отражения структуры явлений;

в) отражения качественных характеристик процессов.

г) содержательного отражения отношений между объектами;

10. Укажите информационные модели, разработка которых регламентируется соглашениями, принятыми в практике создания информационных систем

а) Сетевые модели.

б) Иерархические модели.

+ в) Диаграммы потоков данных.

г) Реляционные модели.

5.2.3. 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 ответам 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.

6 Учебно-методическое обеспечение

6.1 Основная литература

1. Раченко, Т. А. Информационная безопасность : учебно-методическое пособие / Т. А. Раченко. — Тольятти : ТГУ, 2024. — 135 с. — ISBN 978-5-8259-1612-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/427130 (дата обращения: 30.03.2026). — Режим доступа: для авториз. пользователей.

2. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2024. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2082642 (дата обращения: 27.03.2026). – Режим доступа: по подписке.

3. Зенков, А. В. Информационная безопасность и защита информации: учебник для вузов / Зенков А. В.. – 2-е изд., пер. и доп. – Москва : Юрайт, 2025. – 107 с. – ISBN 978-5-534-16388-9. – URL: https://urait.ru/book/informacionnaya-bezopasnost-i-zaschita-informacii-567915 (дата обращения: 30.03.2026). – Текст : электронный.

6.2 Дополнительная литература

1. Чернова, Е. В. Информационная безопасность человека: учебник для вузов / Чернова Е. В.. – 3-е изд., пер. и доп. – Москва : Юрайт, 2025. – 327 с. – ISBN 978-5-534-16772-6. – URL: https://urait.ru/book/informacionnaya-bezopasnost-cheloveka-566457 (дата обращения: 30.03.2026). – Текст : электронный.

2. Щербак, А. В. Информационная безопасность: учебник для вузов / Щербак А. В.. – 2-е изд. – Москва : Юрайт, 2025. – 252 с. – ISBN 978-5-9916-4299-6. – URL: https://urait.ru/book/informacionnaya-

bezopasnost-569267 (дата обращения: 30.03.2026). – Текст : электронный.

3. Баланов, А. Н. Комплексная информационная безопасность : учебное пособие для вузов / А. Н. Баланов. — Санкт-Петербург : Лань, 2024. — 400 с. — ISBN 978-5-507-49250-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/414947 (дата обращения: 30.03.2026). — Режим доступа: для авториз. пользователей.

6.3 Методическая литература

1. Методические рекомендации по организации учебной деятельности обучающихся КузГТУ / ФГБОУ ВО «Кузбас. гос. техн. ун-т им. Т. Ф. Горбачева», Каф. приклад. информ. технологий ; сост. Л. И. Михалева. – Кемерово : КузГТУ, 2017. – 32 с. – URL: http://library.kuzstu.ru/meto.php?n=553 (дата обращения: 30.03.2026). – Текст : электронный.

6.4 Профессиональные базы данных и информационные справочные системы

1. Универсальная полнотекстовая база данных электронных периодических изданий «ИВИС» https://eivis.ru/
2. Электронная библиотечная система «Университетская библиотека онлайн» http://biblioclub.ru/
3. Электронная библиотечная система «Лань» http://e.lanbook.com
4. Электронная библиотека КузГТУ https://library.kuzstu.ru/index.php/punkt-2/podrazdel-21
5. Электронная библиотека Новосибирского государственного технического университета https://clck.ru/UoXpv
6. Электронная библиотечная система «Znanium» https://new.znanium.com/my/documents
7. Справочная правовая система «КонсультантПлюс» http://www.consultant.ru/
8. Электронная библиотека "Эксперт" Системы Технорматив https://gost.online/index.htm
9. Национальная электронная библиотека https://rusneb.ru/

6.5 Периодические издания

1. Безопасность информационных технологий: научный журнал https://eivis.ru/browse/publication/379646
2. Информация и безопасность : научный журнал

7 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

ЭИОС КузГТУ:

a) Электронная библиотека КузГТУ. – Текст: электронный // Научно-техническая библиотека Кузбасского государственного технического университета им. Т. Ф. Горбачева : сайт. – Кемерово, 2001 – . – URL: https://elib.kuzstu.ru/. – Текст: электронный.

b) Портал.КузГТУ : Автоматизированная Информационная Система (АИС) : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://portal.kuzstu.ru/. – Режим доступа: для авториз. пользователей. – Текст: электронный.

c) Электронное обучение : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://el.kuzstu.ru/. – Режим доступа: для авториз. пользователей КузГТУ. – Текст: электронный.

8 Методические указания для обучающихся по освоению дисциплины "Построение моделей угроз информационной безопасности"

Самостоятельная работа обучающегося является частью его учебной деятельности, объемы самостоятельной работы по каждой дисциплине (модулю) практике, государственной итоговой аттестации, устанавливаются в учебном плане.

Самостоятельная работа по дисциплине (модулю), практике организуется следующим образом:

1. До начала освоения дисциплины обучающемуся необходимо ознакомиться с содержанием рабочей программы дисциплины (модуля), программы практики в следующем порядке:

1.1 содержание знаний, умений, навыков и (или) опыта профессиональной деятельности, которые будут сформированы в процессе освоения дисциплины (модуля), практики;

1.2 содержание конспектов лекций, размещенных в электронной информационной среде КузГТУ в порядке освоения дисциплины, указанном в рабочей программе дисциплины (модуля), практики;

1.3 содержание основной и дополнительной литературы.

2. В период освоения дисциплины обучающийся осуществляет самостоятельную работу в следующем порядке:

2.1 выполнение практических и (или) лабораторных работы и (или) отчетов в порядке, установленном в рабочей программе дисциплины (модуля), практики;

2.2 подготовка к опросам и (или) тестированию в соответствии с порядком, установленном в рабочей программе дисциплины (модуля), практики;

2.3 подготовка к промежуточной аттестации в соответствии с порядком, установленном в рабочей программе дисциплины (модуля), практики.

В случае затруднений, возникших при выполнении самостоятельной работы, обучающемуся необходимо обратиться за консультацией к педагогическому работнику. Периоды проведения консультаций устанавливаются в расписании консультаций.

9 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине "Построение моделей угроз информационной безопасности", включая перечень программного обеспечения и информационных справочных систем

Для изучения дисциплины может использоваться следующее программное обеспечение:

1. Ubuntu
2. Libre Office
3. Google Chrome
4. Yandex
5. GIMP
6. 7-zip
7. Open Office
8. Microsoft Windows
9. Microsoft Project
10. Kaspersky Endpoint Security

10 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине "Построение моделей угроз информационной безопасности"

Специально оборудованный кабинет №1147 представляет собой компьютерный класс обеспечивающий практическую подготовку в соответствии с направленностью (профилем) программы магистратуры для научно-исследовательской работы обучающихся, курсового и дипломного проектирования, оснащенный рабочими местами на базе вычислительной техники с набором необходимых для проведения и оформления результатов исследований дополнительных аппаратных и (или) программных средств, а также комплектом оборудования для печати.

Перечень основного оборудования:

Специализированная мебель (столы и стулья); Коммутаторы, Металлические рольставни с пружинным механизмом, белые 1650мм*2270мм; Сейф металлический; Системные блоки ITS (i3-10100/H410M/8 Gb/SSD 240Gb/БП AA500W); Точка доступа D-link; Мониторы 23.6" AOC 24B1H VA 1920x1080 (16:9), 250кд/м2, 5мс, VGA, HDMI, черные; Системные блокиMasteroMiddleMC05, IntelCorei510400 2.9GHz, 8GbRAM, 240GbSSD, DOS, программно-аппаратный комплекс для обнаружения компьютерных атак VipNet, средство доверенной загрузки (СДЗ) Соболь.

Специальное помещение для самостоятельной работы № 1211

Перечень основного оборудования:

специализированная мебель (столы и стулья);

компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду КузГТУ;

проектор, экран настенный моторизованный.

Специальное помещение для самостоятельной работы № 3210

Перечень основного оборудования:

специализированная мебель (столы и стулья);

компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду КузГТУ.

Специально оборудованный кабинет № 1019 представляет собой аудиторию – специальную библиотеку (библиотеку литературы ограниченного доступа), предназначенную для хранения и обеспечения использования в образовательном процессе нормативных и методических документов ограниченного доступа.

Перечень основного оборудования:

Специализированная мебель (столы и стулья).

Специальное помещение № 6308 представляет собой аудиторию (защищаемое помещение) для проведения учебных занятий, в ходе которых до обучающихся доводится информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну. Аттестат соответствия №2601.49.22 от 09.09.2022.

Перечень основного оборудования:

Специализированная мебель (столы и стулья); АРМ, Аттестат соответствия №2601.48.22 от 09.09.2022

11 Иные сведения и (или) материалы

1. Образовательный процесс осуществляется с использованием как традиционных так и современных интерактивных технологий.

В рамках аудиторных занятий применяются следующие интерактивные методы:

- разбор конкретных примеров;
- мультимедийная презентация.

2. Проведение групповых и индивидуальных консультаций осуществляется в соответствии с расписанием консультаций по темам, заявленным в рабочей программе дисциплины, в период освоения дисциплины и перед промежуточной аттестацией с учетом результатов текущего контроля.