

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

Подразделение: институт информационных
технологий, машиностроения и
автотранспорта

Должность: директор института

Дата: 15.09.2026 16:03:59

Дубинкин Дмитрий Михайлович

Рабочая программа дисциплины

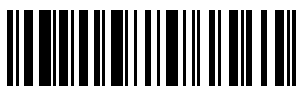
Организация приемочных испытаний системы защиты информации

Направление подготовки 10.04.01 Информационная безопасность
Направленность (профиль) 01 Организация и технология защиты информации

Присваиваемая квалификация
"Магистр"

Формы обучения
очно-заочная

Кемерово 2026 г.



1784088837

Рабочую программу составил:

ПОДПИСАНО ЭП КУЗГТУ

Подразделение: кафедра информационной безопасности

Должность: заведующий кафедрой (к.н.,спд)

Дата: 17.07.2026 10:14:32

Прокопенко Евгения Викторовна

Рабочая программа обсуждена на заседании кафедры информационной безопасности

Протокол № 9 от 03.07.2026

ПОДПИСАНО ЭП КУЗГТУ

Подразделение: кафедра информационной безопасности

Должность: заведующий кафедрой (к.н.,спд)

Дата: 17.07.2026 10:14:51

Прокопенко Евгения Викторовна

Согласовано учебно-методической комиссией по направлению подготовки (специальности)
10.04.01 Информационная безопасность

Протокол № 9 от 03.06.2027

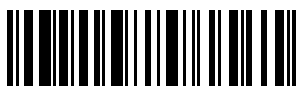
ПОДПИСАНО ЭП КУЗГТУ

Подразделение: кафедра информационной безопасности

Должность: заведующий кафедрой (к.н.,спд)

Дата: 17.07.2026 10:15:10

Прокопенко Евгения Викторовна



1784088837

1 Перечень планируемых результатов обучения по дисциплине "Организация приемочных испытаний системы защиты информации", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:
профессиональных компетенций:

ПК-5 - Способен организовывать и проводить приемочные испытания СЗИ, вводить в эксплуатацию СЗИ

Результаты обучения по дисциплине определяются индикаторами достижения компетенций

Индикатор(ы) достижения:

Способен организовывать и проводить приемочные испытания СЗИ, вводить в эксплуатацию СЗИ

Результаты обучения по дисциплине:

Нормативную базу регламентирующую приемочные испытания СЗИ при вводе в эксплуатацию СЗИ

Умеет организовывать приемочные испытания системы защиты информации

Методами организация приемочных испытаний системы защиты информации

2 Место дисциплины "Организация приемочных испытаний системы защиты информации" в структуре ОПОП магистратуры

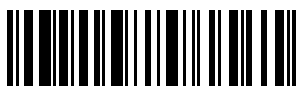
Для освоения дисциплины необходимы знания умения, навыки и (или) опыт профессиональной деятельности, полученные в рамках изучения следующих дисциплин: Управление информационной безопасностью, Организационно-распорядительная документация по обеспечению информационной безопасности, Сертификация средств защиты информации, Построение моделей угроз информационной безопасности, Технологии обеспечения информационной безопасности.

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 "Организация приемочных испытаний системы защиты информации" 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 "Организация приемочных испытаний системы защиты информации" составляет 4 зачетных единицы, 144 часа.

Форма обучения	Количество часов		
	ОФ	ЗФ	ОЗФ
Курс 2/Семестр 3			
Всего часов			144
Контактная работа обучающихся с преподавателем (по видам учебных занятий):			
Аудиторная работа			
Лекции			
Лабораторные занятия			
Практические занятия			24
Внеаудиторная работа			
Индивидуальная работа с преподавателем:			
Консультация и иные виды учебной деятельности			
Самостоятельная работа под руководством преподавателя			40
Самостоятельная работа			44
Форма промежуточной аттестации			экзамен /36



1784088837

4 Содержание дисциплины "Организация приемочных испытаний системы защиты информации", структурированное по разделам (темам)

4.1. Практические (семинарские) занятия

Тема занятия	Трудоемкость в часах	
	ОФ	ОЗФ
Законодательная регламентация приемочных испытаний	4	4
Внедрение системы защиты информации информационной системы	4	4
Аттестация информационной системы и ввод ее в действие	4	4
Составление типовой программы и методики приемочных испытаний системы защиты информации организации	12	12
Итого	24	24

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

Вид СРС	Трудоемкость в часах	
	ОФ	ОЗФ
Ознакомление с содержанием основной и дополнительной литературы, методических материалов, конспектов для подготовки к занятиям	16	16
Оформление отчетов по практическим и(или) лабораторным работам	18	18
Подготовка к промежуточной аттестации	6	6
Итого	40	40
Самостоятельная работа под руководством преподавателя	40	40
Экзамен	36	36

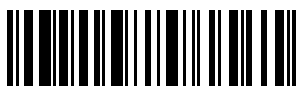
5 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине "Организация приемочных испытаний системы защиты информации"

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



1784088837

Опрос по контрольным вопросам, подготовка отчетов по практическим и (или) лабораторным работам	ПК-5	Способен организовывать и проводить приемочные испытания СЗИ, вводить эксплуатацию СЗИ.	Знать нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации. Уметь организовывать приемочные испытания системы защиты информации. Владеть методами организация приемочных испытаний системы защиты информации. Нормативную базу регламентирующую приемочные испытания СЗИ при вводе в эксплуатацию СЗИ	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.

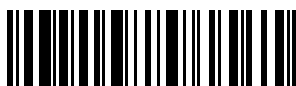
Например:

Содержание вопроса (задания)	Правильный ответ
Коллегиальный орган, назначаемый приказом руководителя для проведения проверки соответствия системы защиты информации (СЗИ) требованиям технического задания и принятия решения о её приемке, называется приемочная _____.	комиссия
Документально зафиксированные сведения о выявленных в ходе испытаний отказах, сбоях или несоответствиях СЗИ проектным решениям называются перечнем _____.	замечаний (или недостатков).

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



1784088837

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		

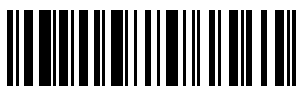
Примерный перечень вопросов на экзамен:

Содержание вопроса (задания)	Правильный ответ
Коллегиальный орган, назначаемый приказом руководителя для проведения проверки соответствия системы защиты информации (СЗИ) требованиям технического задания и принятия решения о её приемке, называется приемочная _____.	комиссия
Документально зафиксированные сведения о выявленных в ходе испытаний отказах, сбоях или несоответствиях СЗИ проектным решениям называются перечнем _____.	замечаний (или недостатков).
Проверка СЗИ, проводимая с целью подтверждения того, что программное обеспечение не было изменено в процессе поставки и установки, называется контролем _____.	целостности
Этап испытаний, проводимый непосредственно перед приемочными испытаниями для определения готовности системы к опытной эксплуатации, называется _____ испытаниями.	предварительными

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;



1784088837

- 75...84 баллов - при правильном ответе на 13-15 вопросов;
- 65...74 баллов - 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-5 Способен организовывать и проводить приемочные испытания СЗИ, вводить в эксплуатацию СЗИ

Содержание вопроса (задания)		Правильный ответ
Кто, как правило, возглавляет приемочную комиссию при организации испытаний системы защиты информации в организации? 1. 1. Представитель компании-поставщика СЗИ. 2. 2. Самый младший по должности сотрудник отдела ИТ. 3. 3. Председатель комиссии (обычно руководитель организации или его заместитель). 4. 4. Сторонний системный интегратор, не участвовавший в проекте.		3
Что должна сделать приемочная комиссия, если в ходе испытаний выявлены критические несоответствия СЗИ требованиям технического задания? 1. 1. Игнорировать их и подписать акт приемки «как есть». 2. 2. Самостоятельно переписать программный код системы. 3. 3. Отразить недостатки в протоколе и направить систему на доработку. 4. 4. Удалить техническое задание и составить новое под текущие функции.		3
Установите соответствие этапов испытаний и их ключевых задач		А - 2, Б - 3, В - 1.
Этап испытаний	Основная задача	
А) Предварительные испытания	1) Оценка готовности системы к постоянной эксплуатации и подписание акта	
Б) Опытная эксплуатация	2) Проверка работоспособности СЗИ и устранение недоработок разработчиком	
В) Приемочные испытания	3) Отработка навыков персонала и проверка стабильности СЗИ в реальных условиях	
Установите соответствие видов документации их назначению		А - 2, Б - 1, В - 3.
Документ	Что определяет или фиксирует	
А) Программа испытаний	1) Описание конкретных шагов и действий для проверки СЗИ	
Б) Методика испытаний	2) Перечень объектов, объем, сроки и условия проведения проверок	
В) Протокол испытаний	3) Результаты выполнения каждой проверки и выявленные отклонения	
Установите правильную последовательность этапов организации приемочных испытаний системы защиты информации: 1. 1. Формирование приемочной комиссии и издание соответствующего приказа. 2. 2. Подготовка испытательного стенда и проверка комплектности СЗИ. 3. 3. Разработка и согласование Программы и методики испытаний (ПМИ). 4. 4. Анализ исходных требований технического задания (ТЗ) и проектных решений.		4, 3, 1, 2.



1784088837

Содержание вопроса (задания)	Правильный ответ
Установите последовательность действий при завершении приемочных испытаний и оформлении результатов: 1. 1. Оформление итогового Акта о приемке СЗИ в эксплуатацию. 2. 2. Составление протоколов по каждому разделу программы испытаний. 3. 3. Устранение разработчиком выявленных замечаний и недостатков (при наличии). 4. 4. Формирование перечня замечаний и предложений по доработке системы.	2, 4, 3, 1.
Коллегиальный орган, назначаемый приказом руководителя для проведения проверки соответствия системы защиты информации (СЗИ) требованиям технического задания и принятия решения о её приемке, называется приемочная _____.	комиссия
Документально зафиксированные сведения о выявленных в ходе испытаний отказах, сбоях или несоответствиях СЗИ проектным решениям называются перечнем _____.	замечаний (или недостатков).
Проверка СЗИ, проводимая с целью подтверждения того, что программное обеспечение не было изменено в процессе поставки и установки, называется контролем _____.	целостности
Этап испытаний, проводимый непосредственно перед приемочными испытаниями для определения готовности системы к опытной эксплуатации, называется _____ испытаниями.	предварительными

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.

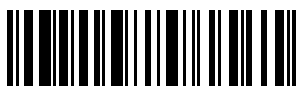
При подготовке ответов на вопросы обучающимся запрещается использование любых электронных и печатных источников информации. В случае обнаружения научно-педагогическим работником факта использования обучающимся при подготовке ответов на вопросы указанные источники информации – оценка результатов текущего 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



1784088837

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.

6 Учебно-методическое обеспечение

6.1 Основная литература

1. Васильев, В. И. Интеллектуальные системы защиты информации : учебное пособие / В. И. Васильев. — 3-е изд., стереотип. — Москва : Машиностроение, 2021. — 172 с. — ISBN 978-5-907104-99-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/192986> (дата обращения: 01.04.2025). — Режим доступа: для авториз. пользователей.

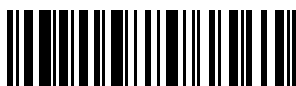
2. Комплексные системы защиты информации на предприятиях : учебное пособие / составители Д. С. Алексеев, О. В. Щекочихин. — Кострома : КГУ, 2021. — 167 с. — ISBN 978-5-8285-1164-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/201884> (дата обращения: 01.04.2025). — Режим доступа: для авториз. пользователей.

3. Бабаш, А. В. Моделирование системы защиты информации. Практикум : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 3-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2025. — 355 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование). — DOI: <https://doi.org/10.29039/01848-4>. - ISBN 978-5-369-01969-6. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2173934> (дата обращения: 07.09.2026). - Режим доступа: по подписке.

4. Петровский, В. И. Принципы построения системы защиты информации на предприятиях различных форм собственности : учебное пособие / В. И. Петровский ; под редакцией В. И. Петровского. — Казань : КНИТУ-КАИ, 2016. — 512 с. — ISBN 978-5-7579-2150-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/149575> (дата обращения: 01.04.2025). — Режим доступа: для авториз. пользователей.

6.2 Дополнительная литература

1. Васильев, В. И. Интеллектуальные системы защиты информации : учебное пособие / В. И.



1784088837

Васильев. — 2-е изд., испр. и доп. . — Москва : Машиностроение, 2013. — 172 с. — ISBN 978-5-94275-667-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/5792> (дата обращения: 01.04.2025). — Режим доступа: для авториз. пользователей.

2. Системы защиты информации в ведущих зарубежных странах : учебное пособие : [16+] / В. И. Аверченков, М. Ю. Рытов, Г. В. Кондрашин, М. В. Рудановский ; науч. ред. В. И. Аверченков. — 5-е изд., стер. — Москва : ФЛИНТА, 2021. — 224 с. : ил., схем. — (Организация и технология защиты информации). — Режим доступа: по подписке. — URL: <https://biblioclub.ru/index.php?page=book&id=93351> (дата обращения: 13.09.2026). — Библиогр.: с. 192-193. — ISBN 978-5-9765-1274-0. — Текст : электронный.

3. Киреева, Н. В. Эффективность системы защиты информации на основе экспертных систем : методические указания / Н. В. Киреева, И. С. Поздняк. — Самара : ПГУТИ, 2021. — 29 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/301109> (дата обращения: 01.04.2025). — Режим доступа: для авториз. пользователей.

4. Лихачева, А. А. Разработка организационной системы защиты информации государственной информационной системы «Бюджет» Министерства финансов Челябинской области / А. А. Лихачева ; Южно-Уральский государственный университет (национальный исследовательский университет). — Челябинск : б.и., 2020. — 118 с. : ил., табл. — Режим доступа: по подписке. — URL: <https://biblioclub.ru/index.php?page=book&id=615432> (дата обращения: 10.09.2026). — Текст : электронный.

5. Кузнецов, А. А. Математическое обоснование эффективности системы защиты информации на объекте информатизации / А. А. Кузнецов ; Севастопольский государственный университет. — Севастополь : б.и., 2021. — 127 с. : ил., схем. — Режим доступа: по подписке. — URL: <https://biblioclub.ru/index.php?page=book&id=617772> (дата обращения: 10.09.2026). — Текст : электронный.

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: 01.04.2025). — Текст : электронный.

6.4 Профессиональные базы данных и информационные справочные системы

1. Электронная библиотечная система «Университетская библиотека онлайн» <http://biblioclub.ru/>
2. Электронная библиотечная система «Лань» <http://e.lanbook.com>
3. Электронная библиотека КузГТУ <https://library.kuzstu.ru/index.php/punkt-2/podrazdel-21>
4. Электронная библиотека Новосибирского государственного технического университета <https://clck.ru/UoXpv>
5. Образовательная платформа «Юрайт» <https://urait.ru/>
6. Электронная библиотечная система «Znaniium» <https://new.znaniium.com/my/documents>
7. Справочная правовая система «КонсультантПлюс» <http://www.consultant.ru/>
8. Национальная электронная библиотека <https://rusneb.ru/>

6.5 Периодические издания

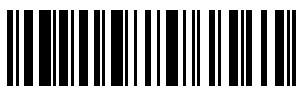
1. Безопасность информационных технологий: научный журнал <https://eivis.ru/browse/publication/379646>
2. Информация и безопасность : научный журнал

7 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

ЭИОС КузГТУ:

а) 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.

б) Портал.КузГТУ : Автоматизированная Информационная Система (АИС) : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. — Кемерово : КузГТУ, [б. г.]. — URL:



1784088837

<https://portal.kuzstu.ru/>. – Режим доступа: для авториз. пользователей. – Текст: электронный.

с) 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 "Организация приемочных испытаний системы защиты информации"

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 "Организация приемочных испытаний системы защиты информации", включая перечень программного обеспечения и информационных справочных систем

Для изучения дисциплины может использоваться следующее программное обеспечение:

1. Libre Office
2. Mozilla Firefox
3. Google Chrome
4. Microsoft Windows
5. ESET NOD32 Smart Security Business Edition
6. Kaspersky Endpoint Security
7. Браузер Спутник

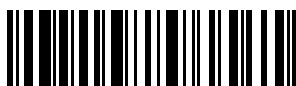
10 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине "Организация приемочных испытаний системы защиты информации"

Лаборатория № 1149 представляет собой лабораторию в области технологий обеспечения информационной безопасности и защищенных информационных систем, оснащенную средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами защиты информации и средствами контроля защищенности информации.

Перечень основного оборудования:

Комплект мебели (столы и стулья). Персональные компьютеры. Сетевое оборудование, технические, программные и программно-аппаратные средства защиты информации и средства контроля защищенности информации.

Моноблок (Intel Core i5-10400 / 8 Gb RAM); горизонт кабельный организатор (25B-1U-02BL); коммутац панель кат.5 (27B-U5-24BL 24 ports); коммутац панель кат.6 (27B-U6-24BL 24 ports); шкаф



1784088837

коммутатор Eurolan (S3000-22U 600x600 мм, перед - стекло, зад - металл, 60F-22-66-31BL); коммутатор управляемый (D-Link DGS-3130-54TS 48 ports); программно-аппаратный комплекс (Infotecs IDS-1000); модуль доверенной загрузки («Соболь-4»); средство активной защиты информации от утечки за счет наводок информ сигнала на цепи заземления и электропитания («Соната-PC3»); точка доступа Wi-fi двухдиапазонная (D-Link DWL-8620AP); патч-корды кат 5 (Eurolan); патч-корды кат 6 (Eurolan);

кабельный тестер (CableMaster-800); коммутатор управляемый (D-Link DES-1210-28 28 ports); коммутатор неуправляемый (D-Link DSS-100E-9P 8+1 ports); маршрутизатор проводной (D-Link DSR-150 8 ports); Wi-Fi маршрутизатор двухдиапазонный (D-Link DWR-980 4 Lan-ports).

Перечень программного обеспечения: Libre Office. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. Браузер Спутник.

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.

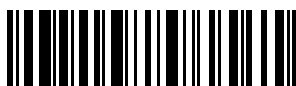
11 Иные сведения и (или) материалы

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.



1784088837