

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 16:02:06

Дубинкин Дмитрий Михайлович

Рабочая программа дисциплины

Организационно-распорядительная документация по обеспечению информационной безопасности

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.



1784080024

Рабочую программу составил:

ПОДПИСАНО ЭП КУЗГТУ

Подразделение: кафедра информационной безопасности

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

Дата: 17.07.2026 10:02:21

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 10:02:38

Прокопенко Евгения Викторовна

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

Протокол № 9 от 03.07.2026

ПОДПИСАНО ЭП КУЗГТУ

Подразделение: кафедра информационной безопасности

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

Дата: 17.07.2026 10:03:13

Прокопенко Евгения Викторовна



1784080024

1 Перечень планируемых результатов обучения по дисциплине "Организационно-распорядительная документация по обеспечению информационной безопасности", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:

общефессиональных компетенций:

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

Результаты обучения по дисциплине определяются индикаторами достижения компетенций

Индикатор(ы) достижения:

Разрабатывает проекты организационно-распорядительных документов по обеспечению информационной безопасности.

Результаты обучения по дисциплине:

Знать источники правовой информации, виды нормативных правовых актов, стандарты в области информационной безопасности.

Уметь анализировать, изучать и обобщать правовую информацию, определять релевантные для профессиональной деятельности нормативные акты, использовать нормативные и методические документы при оформлении технической документации.

Владеть навыками обоснования своих решений на основе действующего законодательства, навыками поиска требуемой информации используя нормативные правовые акты, навыками подготовки проектов организационно-распорядительных документов по обеспечению информационной безопасности.

2 Место дисциплины "Организационно-распорядительная документация по обеспечению информационной безопасности" 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, Построение моделей угроз 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 "Организационно-распорядительная документация по обеспечению 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 "Организационно-распорядительная документация по обеспечению информационной безопасности" составляет 5 зачетных единиц, 180 часов.

Форма обучения	Количество часов		
	ОФ	ЗФ	ОЗФ
Курс 1/Семестр 2			
Всего часов			180
Контактная работа обучающихся с преподавателем (по видам учебных занятий):			
Аудиторная работа			
Лекции			12
Лабораторные занятия			
Практические занятия			12
Внеаудиторная работа			
Индивидуальная работа с преподавателем:			
Консультация и иные виды учебной деятельности			
Самостоятельная работа под руководством преподавателя			86



1784080024

Форма обучения	Количество часов		
	ОФ	ЗФ	ОЗФ
Самостоятельная работа			34
Форма промежуточной аттестации			экзамен /36

4 Содержание дисциплины "Организационно-распорядительная документация по обеспечению информационной безопасности", структурированное по разделам (темам)

4.1. Лекционные занятия

Раздел дисциплины, темы лекций и их содержание	Трудоемкость в часах	
	ОФ	ОЗФ
1. Введение. 1.1 Правовое регулирование в информационной сфере. Обеспечение информационной безопасности организации.	2	2
2. Законодательство об информации и ее защите. 2.1. Законодательство об информации, информационных технологиях и о защите информации. Законодательство о персональных данных.	2	2
3. Интеллектуальная собственность. 3.1 Правовая охрана объектов промышленной собственности. Авторское право. Ноу-хау. 3.2 Особенности правовой охраны программ для ЭВМ и баз данных.	2	2
4. Государственная и коммерческая тайна. 4.1 Законодательство о государственной тайне. Законодательство о коммерческой тайне.	2	2
5. Электронная подпись. 5.1 Законодательство об электронной подписи. 5.2 Организация работы удостоверяющего центра.	2	2
6. Организационное обеспечение информационной безопасности. 6.1 Организационные структуры обеспечения информационной безопасности. 6.2 Корпоративные нормы в области информационной безопасности.	2	2
Итого	12	12

4.2. Практические (семинарские) занятия

Тема занятия	Трудоемкость в часах	
	ОФ	ОЗФ
1. Введение	2	2
2. Законодательство об информации и ее защите	2	2
3. Интеллектуальная собственность	2	2
4. Государственная и коммерческая тайна	2	2
5. Электронная подпись	2	2
6. Организационное обеспечение информационной безопасности	2	2



1784080024

Итого	12	12
--------------	-----------	-----------

4.3 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	10	10
Оформление отчетов по практическим и(или) лабораторным работам	18	18
Подготовка к промежуточной аттестации	6	6
Итого	34	34
Экзамен	36	36
Самостоятельная работа под руководством преподавателя	86	86

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.

5 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине "Организационно-распорядительная документация по обеспечению информационной безопасности"

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) достижений компетенции	Результаты обучения по дисциплине (модулю)	Уровень



1784080024

Опрос по контрольным вопросам, подготовка отчетов по практическим и (или) лабораторным работам	ОПК-3	Разрабатывает проекты организационно-распорядительных документов по обеспечению информационной безопасности	Знать источники правовой информации, виды нормативных правовых актов, стандарты в области информационной безопасности. Уметь анализировать, изучать и обобщать правовую информацию, определять релевантные для профессиональной деятельности нормативные акты, использовать нормативные и методические документы при оформлении технической документации. Владеть навыками обоснования своих решений на основе действующего законодательства, навыками поиска требуемой информации используя нормативные правовые акты, навыками подготовки проектов организационно-распорядительных документов по обеспечению информационной безопасности.	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
Документ, определяющий высокоуровневые цели, принципы и общую стратегию защиты информации в организации, называется _____ информационной безопасности.	Политика
Процедура предварительного рассмотрения и подтверждения согласия с содержанием проекта документа со стороны заинтересованных должностных лиц (юристов, ИТ-директора и др.) называется _____ документа.	Согласование (или Визирование)

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



1784080024

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
Документ, определяющий высокоуровневые цели, принципы и общую стратегию защиты информации в организации, называется _____ информационной безопасности.	Политика
Процедура предварительного рассмотрения и подтверждения согласия с содержанием проекта документа со стороны заинтересованных должностных лиц (юристов, ИТ-директора и др.) называется _____ документа.	Согласование (или Визирование)
Локальный нормативный акт, детально описывающий порядок выполнения конкретных действий пользователем или администратором при работе со средствами защиты информации, называется _____.	Инструкция



1784080024

Совокупность документов, определяющих порядок функционирования системы защиты информации и обязанности персонала, составляет _____ базу обеспечения информационной безопасности организации.	Нормативно-методическую (или Организационно-распорядительную).
--	--

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

Содержание вопроса (задания)		Правильный ответ
Какой документ является верхнеуровневым в иерархии ОРД организации и определяет общие цели, принципы и стратегию обеспечения информационной безопасности? 1. 1. Инструкция по смене паролей. 2. 2. Журнал учета электронных носителей. 3. 3. Политика информационной безопасности. 4. 4. Акт об уничтожении документов.		3
При разработке проекта документа «Инструкция по антивирусной защите», какой раздел является обязательным для описания действий сотрудника при обнаружении признаков заражения ПК? 1. 1. История создания антивирусного ПО. 2. 2. Порядок действий при возникновении инцидента. 3. 3. Технические характеристики процессора. 4. 4. Список контактов поставщика оборудования.		2
Установите соответствие категорий документов и их назначения		А - 2, Б - 3, В - 1.
Категория документа	Основное назначение в системе ИБ	
А) Политика ИБ	1) Описание пошаговых действий сотрудника при возникновении инцидента	
Б) Регламент	2) Определение общих целей, принципов и стратегию защиты информации	
В) Инструкция	3) Описание порядка выполнения конкретного технологического процесса	
Установите соответствие документов по ИБ и их содержания		А - 2, Б - 3, В - 1.
Название документа	Ключевое содержание	
А) Перечень ПДн	1) Правила использования сменных носителей информации	
Б) Модель угроз	2) Список категорий данных, обрабатываемых в организации	
В) Инструкция по антивирусной защите	3) Описание возможных каналов утечки и типов нарушителей	



1784080024

Содержание вопроса (задания)	Правильный ответ
Установите правильную последовательность жизненного цикла локального нормативного акта по информационной безопасности: 1. 1. Согласование проекта документа с заинтересованными подразделениями (ИТ, юристы, кадры). 2. 2. Подготовка проекта текста документа ответственным исполнителем. 3. 3. Ознакомление сотрудников организации с документом под роспись. 4. 4. Утверждение документа приказом руководителя организации.	2, 1, 4, 3.
Расположите типы документов по информационной безопасности в порядке убывания их юридической силы и иерархии в организации: 1. 1. Инструкция администратора конкретной информационной системы. 2. 2. Приказ руководителя о введении режима защиты информации. 3. 3. Политика информационной безопасности организации. 4. 4. Регламент взаимодействия при возникновении инцидентов ИБ.	3, 2, 4, 1.

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.



1784080024

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. Алёшкин, А. С. Аппаратные и программные средства поиска уязвимостей при моделировании и эксплуатации информационных систем (обеспечение информационной безопасности) : учебное пособие / А. С. Алёшкин, С. А. Лесько, Д. О. Жуков. — Москва : РТУ МИРЭА, 2020. — 152 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/167600> (дата обращения: 07.09.2026). — Режим доступа: для авториз. пользователей.

2. Дронов, В. Ю. Бизнес-процесс «Обеспечение информационной безопасности организации» : учебное пособие / В. Ю. Дронов, Г. А. Дронова. — Новосибирск : НГТУ, 2021. — 76 с. — ISBN 978-5-7782-4537-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/306350> (дата обращения: 07.09.2026). — Режим доступа: для авториз. пользователей.

3. Документальное обеспечение информационной безопасности : учебное пособие / составители Е. Е. Смычков [и др.]. — Севастополь : СевГУ, 2022. — 142 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/261899> (дата обращения: 07.09.2026). — Режим доступа: для авториз. пользователей.

4. Комплексное обеспечение информационной безопасности автоматизированных систем : лабораторный практикум : [16+] / авт.-сост. М. А. Лапина, Д. М. Марков, Т. А. Гиш, М. В. Песков [и др.]. — Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2016. — 242 с. : ил. — Режим доступа: по подписке. — URL: <https://biblioclub.ru/index.php?page=book&id=458012> (дата обращения: 09.09.2026). — Библиогр. в кн. — Текст : электронный.

5. Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии : учебник / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2022. — 344 с. — ISBN 978-5-8114-3940-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/207095> (дата обращения: 07.09.2026). — Режим доступа: для авториз. пользователей.

6. Прокопенко, Е. В. Категорирование объектов критической информационной инфраструктуры : учебное пособие / Е. В. Прокопенко, В. О. Коротин. — Кемерово : КузГТУ имени Т.Ф. Горбачева, 2025. — 112 с. — ISBN 978-5-00137-535-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/516391> (дата обращения: 07.09.2026). — Режим доступа: для авториз.



1784080024

пользователей.

6.2 Дополнительная литература

1. Медведев, Н. В. Дипломное проектирование по специальности «Комплексное обеспечение информационной безопасности автоматизированных систем» : методические указания : методическое пособие : [16+] / Н. В. Медведев, П. М. Квасов ; под ред. В. А. Матвеева ; Московский государственный технический университет им. Н.Э. Баумана. – Москва : МГТУ им. Н.Э. Баумана, 2011. – 80 с. : табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=256990> (дата обращения: 12.09.2026). – Текст : электронный.

2. Комплексное обеспечение информационной безопасности автоматизированных систем : учебное пособие / составители М. А. Лапина [и др.]. – Ставрополь : СКФУ, 2016. – 242 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/book/155111> (дата обращения: 07.09.2026). – Режим доступа: для авториз. пользователей.

3. Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии / М. В. Тумбинская, М. В. Петровский. – 2-е изд., стер. – Санкт-Петербург : Лань, 2022. – 344 с. – ISBN 978-5-507-45046-6. – Текст : электронный // Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/book/256133> (дата обращения: 07.09.2026). – Режим доступа: для авториз. пользователей.

4. Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии : учебник / М. В. Тумбинская, М. В. Петровский. – Санкт-Петербург : Лань, 2019. – 344 с. – ISBN 978-5-8114-3940-9. – Текст : электронный // Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/book/125739> (дата обращения: 07.09.2026). – 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: 07.09.2026). – 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. Справочная правовая система «КонсультантПлюс» <http://www.consultant.ru/>
7. 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: <https://portal.kuzstu.ru/>. – Режим доступа: для авториз. пользователей. – Текст: электронный.



1784080024

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 "Организационно-распорядительная документация по обеспечению 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 "Организационно-распорядительная документация по обеспечению информационной безопасности", включая перечень программного обеспечения и информационных справочных систем

Для изучения дисциплины может использоваться следующее программное обеспечение:

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

10 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине "Организационно-распорядительная документация по обеспечению 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



1784080024

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) Сობоль.

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.



1784080024