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

Нормативные требования по защите информации

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 "Нормативные требования по защите информации", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:

общепрофессиональных компетенций:

ОПК-7.2. - Способен разрабатывать методики и тесты для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации;

Результаты обучения по дисциплине определяются индикаторами достижения компетенций

Индикатор(ы) достижения:

Разрабатывает методики и тесты для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации.

Результаты обучения по дисциплине:

Знать методики и тесты для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации.

Уметь использовать методики и проводить тесты для анализа степени защищенности информационной системы, определять её соответствие нормативным требованиям по защите информации.

Владеть знаниями документации Федеральной службы по техническому и экспортному контролю (ФСТЭК России) по защите информации.

2 Место дисциплины "Нормативные требования по защите информации" в структуре ОПОП специалитета

Для освоения дисциплины необходимы знания умения, навыки и (или) опыт профессиональной деятельности, полученные в рамках изучения следующих дисциплин: Информационные угрозы, Классификация защищаемой информации и информационных систем.

В области 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 "Нормативные требования по защите 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 "Нормативные требования по защите информации" составляет 3 зачетных единицы, 108 часов.

Форма обучения	**Количество часов**		
	ОФ	**ЗФ**	**ОЗФ**
Курс 2/Семестр 3			
Всего часов	108		
Контактная работа обучающихся с преподавателем (по видам учебных занятий):			
Аудиторная работа			
Лекции	16		
Лабораторные занятия			
Практические занятия	32		
Внеаудиторная работа			
Индивидуальная работа с преподавателем:			
Консультация и иные виды учебной деятельности			
Самостоятельная работа	24		
Форма промежуточной аттестации	экзамен /36		

4 Содержание дисциплины "Нормативные требования по защите информации", структурированное по разделам (темам)

4.1. Лекционные занятия

Раздел дисциплины, темы лекций и их содержание	**Трудоемкость в часах**
	ОФ
1. Характеристика систем стандартизации в области защиты информации.	2
2. Оценочные стандарты и технические спецификации.	2
3. Информационная безопасность информационных систем.	4
4. Европейские критерии безопасности информационных технологий.	4
5. Документы Федеральной службы по техническому и экспортному контролю (ФСТЭК России) по защите информации.	4
Итого	**16**

4.2. Практические занятия

Наименование работы	**Трудоемкость в часах**
	ОФ
1. Характеристика систем стандартизации в области защиты информации.	6
2. Оценочные стандарты и технические спецификации.	6
3. Европейские критерии безопасности информационных технологий.	8
4. Документы Федеральной службы по техническому и экспортному контролю (ФСТЭК России) по защите информации.	12
Итого	**32**

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

Наименование работы Вид СРС	**Трудоемкость в часах**
	ОФ
Ознакомление с содержанием основной и дополнительной литературы, методических материалов, конспектов лекций для подготовки к занятиям	8
Оформление отчетов по практическим и(или) лабораторным работам	10
Подготовка к промежуточной аттестации	6
Итого	**24**
Экзамен	36

5 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине "Нормативные требования по защите информации"

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 или тестирование, подготовка отчетов по практическим и(или) лабораторным работам	ОПК-7.2. - Способен разрабатывать методики и тесты для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации	Разрабатывает методики и тесты для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации.	**Знать** методики и тесты для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации. **Уметь** использовать методики и проводить тесты для анализа степени защищенности информационной системы, определять её соответствие нормативным требованиям по защите информации. **Владеть** знаниями документации Федеральной службы по техническому и экспортному контролю (ФСТЭК России) по защите информации.	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. Типовые 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 дисциплине будет заключаться в опросе обучающихся по контрольным вопросам или тестирование по разделу дисциплины, оформлении оформлении отчетов по практическим и(или) лабораторным работам.

Опросе обучающихся по контрольным вопросам или тестирование по разделу дисциплины

Обучающийся отвечает на 2 вопроса, либо отвечает на 10 тестовых заданий.

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

Критерии оценивания при тестировании:

- 100 баллов – при правильном и полном ответе на 10 вопросов;
- 85…99 баллов – при правильном ответе на 8-9 вопросов;
- 75…84 баллов – при правильном ответе на 7 вопросов;
- 65…74 баллов – правильном ответе на 5-6 вопросов
- 25…64 – при правильном ответе только на 4 вопроса;
- 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. Характеристика систем стандартизации в области защиты информации.

1. Понятие системы стандартизации
2. В соответствии с какими принципами осуществляется стандартизация?
3. Какими характеристиками должна обладать современная система стандартизации?
4. Каков государственный статус Российской системы стандартизации?
5. Какой характер стали носить правила разработки стандартов со вводом в действие С 1 июля 2003 г. Федерального закона «О техническом регулировании»?

2. Оценочные стандарты и технические спецификации.

1. В чем различие между оценочными стандартами и техническими спецификациями?
2. Какой документ был первым оценочным стандартом в области ИТ и ИБ?
3. Что описывает техническая спецификация X.800 ?
4. Для каких целей может быть использован стандарт "Канадские критерии" с точки зрения ИБ?
5. Какие существуют спецификации Internet-сообщества?

3. Информационная безопасность информационных систем.

1. Из каких основных аспектов формируется информационная безопасность или информационная защищенность ИС?
2. За счет каких основных механизмов защиты обеспечивается информационная безопасность ИС?
3. Для каких объектов ИС необходимо обеспечить ИБ в первую очередь?
4. Какими методами возможно обеспечить ИБ в корпоративной ИС?
5. Как убедиться в эффективности мер обеспечения ИБ?

4. Европейские критерии безопасности информационных технологий.

1. Какими странами был инициирован выход Европейских критериев безопасности информационных технологий?
2. В чем главная ценность документа «Европейские критерии»?
3. Какие задачи средств информационной безопасности рассматриваются в документе «Европейские критерии»?
4. В чем наблюдается взаимосвязь «Европейских критериев» и «Оранжевой книги»?
5. Какие группы критериев описаны в «Европейских критериях» с подробной разбивкой по 10 классам?

5. Документы Федеральной службы по техническому и экспортному контролю (ФСТЭК России) по защите информации.

1. Что описывает нормативно-правовой акт «Приказ ФСТЭК России от 31 августа 2010 г. N 489» ?
2. Что описывает нормативно-правовой акт «Приказ ФСТЭК России от 11 февраля 2013 г. N 17» ?
3. Какой приказ ФСТЭК регламентирует защиту персональных данных при обработке их в ИС: устанавливает перечень мер безопасности и раскрывает их содержание?
4. Какой приказ ФСТЭК регламентирует работу по защите информации в АС, управляющими опасными производственными и технологическими процессами на важных и потенциально опасных объектах?
5. Какой недостаток характерен для всех документов как ФСТЭК, так и большинства других законодательных документов?

Примерный перечень тестовых заданий:

1. Характеристика систем стандартизации в области защиты информации.

1. Какими характеристиками должна обладать современная система стандартизации? выбрать все верные

сбалансированная
актуальная
тиражируемая
формализуемая

2. Какой государственный статус имеет Российская система стандартизации?

национальный
государственный
федеральный

3. Какой характер стали носить правила разработки стандартов с вводом в действие С 1 июля 2003 г. Федерального закона «О техническом регулировании»?

обязательный
добровольный
рекомендуемый
принудительный

2. Оценочные стандарты и технические спецификации.

1. В оценочном стандарте "Оранжевая книга" фигурируют понятия: выбрать все верные

ядро безопасности
периметр безопасности
центр безопасности

2. К какому типу нормативных документов относится X.800 ?

к оценочному стандарту
к технической спецификации

3. Для каких целей может быть использован стандарт "Канадские критерии" с точки зрения ИБ? выбрать все верные

для разработки требований безопасности
для спецификаций средств защиты
для проектирования ИС

для нормативно-правовой защиты информации

3. Информационная безопасность информационных систем.

1. Основные объекты информационной безопасности в ИС:

Компьютерные сети, базы данных
Информационные системы, психологическое состояние пользователей
Бизнес-ориентированные, коммерческие системы

2. К основным принципам обеспечения информационной безопасности ИС относится:

Экономической эффективности системы безопасности
Многоплатформенной реализации системы
Усиления защищенности всех звеньев системы

3. Принципом информационной безопасности ИС является принцип недопущения:

Неоправданных ограничений при работе в сети (системе)
Рисков безопасности сети, системы
Презумпции секретности

4. Европейские критерии безопасности информационных технологий.

1. В "Гармонизированных критериях Европейских стран" фигурируют понятия: выбрать все верные

цель оценки
система оценки
объект оценки

2. В чем главная ценность документа «Европейские критерии»? выбрать все верные

введение понятия «адекватность средств защиты»
определение шкалы для критериев адекватности
является более современной альтернативой для «оранжевой книги»
определено понятие информационной угрозы и шкала для ее оценки

3. Какие группы критериев описаны в «Европейских критериях» с подробной разбивкой по 10 классам? выбрать все верные

функциональные
адекватности
технические
организационные
концептуальные

5. Документы Федеральной службы по техническому и экспортному контролю (ФСТЭК России) по защите информации.

1. Что описывает нормативно-правовой акт «Приказ ФСТЭК России от 31 августа 2010 г. N 489» ?

требования к защите информации, обрабатываемой в ИС общего пользования
требования об обработке и защите информации, не являющейся гостайной, в ГИС;

2. Какой приказ ФСТЭК регламентирует защиту персональных данных при обработке их в ИС: устанавливает перечень мер безопасности и раскрывает их содержание?

Приказ ФСТЭК России от 18 февраля 2013 г. N 21
Приказ ФСТЭК России от 14 марта 2014 г. N 31

3. Какой недостаток характерен для всех документов как ФСТЭК, так и большинства других законодательных документов?

слишком теоретизирован
слишком большой объем текста
отстает от реалий в сфере кибербезопасности
опережает реалии в сфере кибербезопасности

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 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 или пройденное тестирование.
зачтенные отчеты обучающихся по лабораторным и(или) практическим работам;

На экзамене обучающийся отвечает на 2 вопроса, либо отвечает на 20 тестовых заданий

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	
	не зачтено		зачтено		

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 – 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		Хорошо	Хорошо	Отлично
	не зачтено		зачтено		

Примерный перечень вопросов на экзамен:

1. Понятие системы стандартизации
2. В соответствии с какими принципами осуществляется стандартизация?
3. Какими характеристиками должна обладать современная система стандартизации?
4. Каков государственный статус Российской системы стандартизации?
5. Какой характер стали носить правила разработки стандартов со вводом в действие С 1 июля 2003 г. Федерального закона «О техническом регулировании»?

6. В чем различие между оценочными стандартами и техническими спецификациями?
7. Какой документ был первым оценочным стандартом в области ИТ и ИБ?
8. Что описывает техническая спецификация X.800 ?
9. Для каких целей может быть использован стандарт "Канадские критерии" с точки зрения ИБ?
10. Какие существуют спецификации Internet-сообщества?
11. Из каких основных аспектов формируется информационная безопасность или информационная защищенность ИС?
12. За счет каких основных механизмов защиты обеспечивается информационная безопасность ИС?
13. Для каких объектов ИС необходимо обеспечить ИБ в первую очередь?
14. Какими методами возможно обеспечить ИБ в корпоративной ИС?
15. Как убедиться в эффективности мер обеспечения ИБ?
16. Какими странами был инициирован выход Европейских критериев безопасности информационных технологий?
17. В чем главная ценность документа «Европейские критерии»?
18. Какие задачи средств информационной безопасности рассматриваются в документе «Европейские критерии»?
19. В чем наблюдается взаимосвязь «Европейских критериев» и «Оранжевой книги»?
20. Какие группы критериев описаны в «Европейских критериях» с подробной разбивкой по 10 классам?
21. Что описывает нормативно-правовой акт «Приказ ФСТЭК России от 31 августа 2010 г. N 489» ?
22. Что описывает нормативно-правовой акт «Приказ ФСТЭК России от 11 февраля 2013 г. N 17» ?
23. Какой приказ ФСТЭК регламентирует защиту персональных данных при обработке их в ИС: устанавливает перечень мер безопасности и раскрывает их содержание?
24. Какой приказ ФСТЭК регламентирует работу по защите информации в АС, управляющими опасными производственными и технологическими процессами на важных и потенциально опасных объектах?
25. Какой недостаток характерен для всех документов как ФСТЭК, так и большинства других законодательных документов?

Примерный перечень тестовых заданий на экзамен:

1. Какими характеристиками должна обладать современная система стандартизации? выбрать все верные

сбалансированная
актуальная
тиражируемая
формализуемая

2. Какой государственный статус имеет Российская система стандартизации?

национальный
государственный
федеральный

3. Какой характер стали носить правила разработки стандартов с вводом в действие С 1 июля 2003 г. Федерального закона «О техническом регулировании»?

обязательный
добровольный
рекомендуемый
принудительный

4. В оценочном стандарте "Оранжевая книга" фигурируют понятия: выбрать все верные

ядро безопасности
периметр безопасности
центр безопасности

5. К какому типу нормативных документов относится X.800 ?

к оценочному стандарту
к технической спецификации

6. Для каких целей может быть использован стандарт "Канадские критерии" с точки зрения ИБ? выбрать все верные

для разработки требований безопасности
для спецификаций средств защиты
для проектирования ИС
для нормативно-правовой защиты информации

7. Основные объекты информационной безопасности в ИС:

Компьютерные сети, базы данных
Информационные системы, психологическое состояние пользователей
Бизнес-ориентированные, коммерческие системы

8. К основным принципам обеспечения информационной безопасности ИС относится:

Экономической эффективности системы безопасности
Многоплатформенной реализации системы
Усиления защищенности всех звеньев системы

9. Принципом информационной безопасности ИС является принцип недопущения:

Неоправданных ограничений при работе в сети (системе)
Рисков безопасности сети, системы
Презумпции секретности

10. В "Гармонизированных критериях Европейских стран" фигурируют понятия: выбрать все верные

цель оценки
система оценки
объект оценки

11. В чем главная ценность документа «Европейские критерии»? выбрать все верные

введение понятия «адекватность средств защиты»
определение шкалы для критериев адекватности
является более современной альтернативой для «оранжевой книги»
определено понятие информационной угрозы и шкала для ее оценки

12. Какие группы критериев описаны в «Европейских критериях» с подробной разбивкой по 10 классам? выбрать все верные

функциональные
адекватности
технические
организационные
концептуальные

13. Что описывает нормативно-правовой акт «Приказ ФСТЭК России от 31 августа 2010 г. N 489» ?

требования к защите информации, обрабатываемой в ИС общего пользования
требования об обработке и защите информации, не являющейся гостайной, в ГИС;

14. Какой приказ ФСТЭК регламентирует защиту персональных данных при обработке их в ИС: устанавливает перечень мер безопасности и раскрывает их содержание?

Приказ ФСТЭК России от 18 февраля 2013 г. N 21
Приказ ФСТЭК России от 14 марта 2014 г. N 31

15. Какой недостаток характерен для всех документов как ФСТЭК, так и большинства других законодательных документов?

слишком теоретизирован

слишком большой объем текста
отстает от реалий в сфере кибербезопасности
опережает реалии в сфере кибербезопасности

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. Аверченков, В. И. Аудит информационной безопасности : учебное пособие : [16+] / В. И. Аверченков. – 4-е изд., стер. – Москва : ФЛИНТА, 2021. – 269 с. : ил., схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=93245 (дата обращения: 13.04.2026). – Библиогр. в кн. – ISBN 978-5-9765-1256-6. – Текст : электронный.

2. Дронова, Г. А. Аттестация и аудит информационной безопасности : учебно-методическое пособие : [16+] / Г. А. Дронова ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2016. – 19 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=575351 (дата обращения: 10.04.2026). – Библиогр. в кн. – ISBN 978-5-7782-3114-6. – Текст : электронный.

6.2 Дополнительная литература

1. Ситнов, А. А. Аудит информационной инфраструктуры : учебно-практическое пособие / А. А. Ситнов. – Москва : Евразийский открытый институт, 2011. – 143 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=90796 (дата обращения: 13.04.2026). – ISBN 978-5-374-00042-9. – Текст : электронный.

2. Аудит информационной безопасности органов исполнительной власти : учебное пособие : [16+] / В. И. Аверченков, М. Ю. Рытов, А. В. Кувыклин, М. В. Рудановский. – 5-е изд., стер. – Москва : ФЛИНТА, 2021. – 100 с. : ил., схем., табл. – (Организация и технология защиты информации). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=93259 (дата обращения: 13.04.2026). – Библиогр.: с. 83-84. – ISBN 978-5-9765-1277-1. – Текст : электронный.

6.3 Методическая литература

1. Защита информации : методические материалы для обучающихся специальности 10.05.03 "Информационная безопасность автоматизированных систем" очной формы обучения / ФГБОУ ВО "Кузбас. гос. техн. ун-т им. Т. Ф. Горбачева", Каф. информ. безопасности ; сост.: Е. В. Прокопенко, И. В. Чичерин. – Кемерово : КузГТУ, 2018. – 56 с. – URL: http://library.kuzstu.ru/meto.php?n=4637 (дата обращения: 23.03.2026). – Текст : электронный.

6.4 Профессиональные базы данных и информационные справочные системы

1. База данных Springer Materials http://materials.springer.com/
2. База данных zbMath https://zbmath.org/
3. Цифровая библиотека IPRsmart https://ipr-smart.ru/
4. Электронная библиотечная система «Университетская библиотека онлайн» http://biblioclub.ru/
5. Электронная библиотечная система «Лань» http://e.lanbook.com
6. Электронная библиотека КузГТУ https://library.kuzstu.ru/index.php/punkt-2/podrazdel-21
7. Электронная библиотека Новосибирского государственного технического университета https://clck.ru/UoXpv
8. Образовательная платформа «Юрайт» https://urait.ru/

9. Справочная правовая система «КонсультантПлюс» http://www.consultant.ru/
10. Электронная библиотека "Эксперт" Системы Технорматив https://gost.online/index.htm
11. Национальная электронная библиотека https://rusneb.ru/
12. Базы данных Springer Journals, Springer eBooks https://link.springer.com/

6.5 Периодические издания

1. Безопасность информационных технологий: научный журнал https://eivis.ru/browse/publication/379646
2. Вестник Кузбасского государственного технического университета : научно-технический журнал https://vestnik.kuzstu.ru/
3. Защита информации. Инсайд: информационно-методический журнал https://eivis.ru/browse/publication/122426
4. 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 "Нормативные требования по защите 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 "Нормативные требования по защите информации", включая перечень программного обеспечения и информационных справочных

систем

Для изучения дисциплины может использоваться следующее программное обеспечение:
1. Mozilla Firefox
2. Google Chrome
3. 7-zip
4. Microsoft Windows
5. ESET NOD32 Smart Security Business Edition
6. Microsoft Project
7. Kaspersky Endpoint Security
8. Браузер Спутник

10 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине "Нормативные требования по защите информации"

Для реализации программы учебной дисциплины предусмотрены специальные помещения:

1. Помещения для самостоятельной работы обучающихся должны оснащенные компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа к электронной информационно-образовательной среде Организации.

2. Учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

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.