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

Организационное и правовое обеспечение информационной безопасности

Направление подготовки 10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль) Анализ безопасности информационных систем

Присваиваемая квалификация «Специалист по защите информации»

Формы обучения: очная

Год набора 2026

Новокузнецк 2026 г.

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

Протокол № 6 от 29.05.2026

Зав. Кафедрой ИТиЭД _____ В. В. Шарлай
подпись

СОГЛАСОВАНО:

Заместитель директора по УР _____ Т. А. Евсина
подпись

1 Перечень планируемых результатов обучения по дисциплине "Организационное и правовое обеспечение информационной безопасности", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:

общепрофессиональных компетенций:

ОПК-5 - Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;

ОПК-6 - Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

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:

Применяет нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации

Организует защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

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

Результаты обучения по дисциплине:

Знать основы российской правовой системы и законодательства, правового статуса личности, организации деятельности органов государственной власти Российский Федерации по защите информации; виды и степень ответственности за правонарушения и преступления в информационной сфере.

Знать характеристику основных отраслей российского права, правовые основы обеспечения национальной безопасности РФ; основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации.

Знать порядок работы с персоналом по вопросам обеспечения защиты информации ограниченного доступа, проведения мероприятий по физической и технической защите конфиденциальной информации, организации службы безопасности предприятия; правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях.

Уметь применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; анализировать правовые акты и осуществлять правовую оценку информации.

Уметь определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; предпринимать необходимые меры по восстановлению нарушенных прав.

Уметь разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации; организовывать работы по проверке кандидатов на должность, текущую работу с персоналом по обеспечению информационной безопасности.

Владеть навыками поиска нормативной правовой информации. необходимой для профессиональной деятельности навыками работы с нормативными правовыми актами.

Владеть навыками организации охраны объектов информатизации и обеспечения режима секретности, организации и управления деятельностью службы защиты информации на предприятии.

Владеть навыками работы с персоналом, принятия организационно-управленческих решений, в том числе в нестандартных ситуациях в целях обеспечения информационной безопасности.

2 Место дисциплины "Организационное и правовое обеспечение информационной безопасности" в структуре ОПОП специалитета

Для освоения дисциплины необходимы знания умения, навыки и (или) опыт профессиональной деятельности, полученные в рамках изучения следующих дисциплин: Введение в специальность, Основы информационной безопасности, Нормативные требования по защите информации, Основы информатики, организации ЭВМ, вычислительных и информационных систем, Информационные угрозы, Классификация защищаемой информации и информационных систем.

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 "Организационное и правовое обеспечение 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 "Организационное и правовое обеспечение информационной безопасности" составляет 3 зачетных единицы, 108 часов.

Форма обучения	**Количество часов**		
	ОФ	**ЗФ**	**ОЗФ**
Курс 2/Семестр 4			
Всего часов	108		
Контактная работа обучающихся с преподавателем (по видам учебных занятий):			
Аудиторная работа			
Лекции			
Лабораторные занятия			
Практические занятия	48		
Внеаудиторная работа			
Индивидуальная работа с преподавателем:			
Консультация и иные виды учебной деятельности			
Самостоятельная работа под руководством преподавателя	32		
Самостоятельная работа	28		
Форма промежуточной аттестации	зачет		

4 Содержание дисциплины "Организационное и правовое обеспечение информационной безопасности", структурированное по разделам (темам)

4.1. Лекционные занятия

Раздел дисциплины, темы лекций и их содержание	**Трудоемкость в часах**
	ОФ
1. Организационное обеспечение информационной безопасности.	
1.1. Информационные отношения как объект правового регулирования. Законодательство Российской Федерации в области информационной безопасности	2
1.2. Правовой режим защиты государственной тайны и информации ограниченного доступа	2
1.3. Правовая охрана результатов интеллектуальной деятельности	4

1.4. Преступления в сфере компьютерной информации	2
1.5. Понятие организационной защиты информации	2
1.6. Подбор сотрудников на должности, связанные с работой с конфиденциальной информацией, и текущая работа с ним.	4
1.7. Допуск и доступ к государственной, служебной тайнам и персональным данным сотрудников	2
1.8. Организация служебного расследования по фактам разглашения и утечки конфиденциальной информации.	2
1.9. Требования к помещениям и хранилищам, в которых ведутся закрытые работы и хранятся конфиденциальные документы и изделия.	2
1.10. Организация охраны территории, зданий, помещений и сотрудников. Организация пропускного и внутриобъектового режимов	2
2. Правовое обеспечение информационной безопасности.	
2.11. Место информационной безопасности в системе информационного права	2
2.12. Информационная безопасность	2
2.13. Ответственность за нарушение информационного законодательства	4
Итого	**32**

4.2 Практические (семинарские) занятия

Тема занятия	**Трудоемкость в часах**
	ОФ
1 (2). Правовой режим защиты государственной тайны. Правовые режимы защиты информации ограниченного доступа	2
2 (3). Правовая охрана результатов интеллектуальной деятельности.	2
3 (6). Подбор сотрудников на должности, связанные с работой с конфиденциальной информацией, и текущая работа с ним	2
4 (7). Допуск и доступ к государственной, служебной тайнам и персональным данным сотрудников.	2
5 (8). Организация служебного расследования по фактам разглашения и утечки конфиденциальной информации.	2
6 (9). Требования к помещениям и хранилищам, в которых ведутся закрытые работы и хранятся конфиденциальные документы и изделия	2
7 (10). Организация охраны территории, зданий, помещений и сотрудников. Организация пропускного и внутриобъектового режимов	2

8 (11). Место информационной безопасности в системе информационного права: 8.1. Право и его роль в регулировании комплекса отношений в информационной сфере. Понятие об информационном объекте и его элементах. Правовая информация, Официальная правовая информация, информация индивидуально правовая, неофициальная правовая информация. Юридические особенности и свойства информации (2) 8.2. Информационные правоотношения. Объекты и субъекты информационных правоотношений. Виды информационно-правовых норм: по содержанию, по масштабу действия. Система информационного права: общая часть; особенная часть. Принципы информационного права (2)	4

9 (12). Информационная безопасность. 9.1. Понятие информационной безопасности личности. Соблюдение конституционных прав и свобод человека и гражданина в области информационных правоотношений. Запрет цезуры. Ограничения использования информации о частной жизни. Гарантии информационных прав граждан. Право на судебную защиту. Информационная безопасность общества Понятие информационной безопасности общества. Правовое регулирование средств информатизации, телекоммуникации и связи. Правовое регулирование единого информационного пространства. Информационная безопасность государства. Понятие информационной безопасности государства. Обеспечение защиты информационных ресурсов от несанкционированного доступа. Обеспечение безопасности информационных и телекоммуникационных систем (2). 9.2. Понятие правового режима защиты государственной тайны. Государственная тайна как особый вид защищаемой информации и ее характерные признаки. Реквизиты носителей сведений, составляющих государственную тайну. Принципы, механизм и процедура отнесения сведений к государственной тайне, их засекречивания и рассекречивания. Органы защиты государственной тайны и их компетенция. Порядок допуска и доступа к государственной тайне. Иные меры по обеспечению сохранности сведений, составляющих государственную тайну (режим секретности как основной порядок деятельности в сфере защиты государственной тайны). Перечень и содержание мер, направленных на защиту государственной тайны. Система контроля за состоянием защиты государственной тайны (4) 9.3. Правовая регламентация лицензионной деятельности в области защиты информации. Объекты лицензирования в сфере защиты информации. Участники лицензионных отношений в сфере защиты информации. Специальные экспертизы и государственная аттестация руководителей. Органы лицензирования и их полномочия. Контроль за соблюдением лицензиатами условий ведения деятельности (4). 9.4. Правовая регламентация сертификационной деятельности в области защиты информации. Режимы сертификации. Объекты сертификационной деятельности (сертификации). Органы сертификации и их полномочия. Правовые основы защиты информации с использованием технических средств (защиты от технических разведок, применения и разработки шифровальных средств, применения электронно-цифровой подписи и т.д.) (4). 9.5. Законодательство РФ об интеллектуальная собственности. Понятие интеллектуальной собственности. Объекты и субъекты авторского права. Исключительные авторские права. Смежные права. Правовая охрана программ для ЭВМ, баз данных и топологий интегральных микросхем. Защита авторских и смежных прав. Основы патентных правоотношений. Условия патентоспособности. Объекты изобретения, связанные с электронно-вычислительной техникой и информационными технологиями. Авторы изобретений и патентообладатели. Механизм патентования. Защита прав патентообладателей и авторов. Особенности договорных отношений в области информационной безопасности. Правовое регулирование взаимоотношений администрации и персонала в области обеспечения информационной безопасности (4). 9.6. Правовой режим персональных данных Правовые основы защиты персональных данных в Конституции РФ. Основные положения Европейской конвенции о защите личности в связи с автоматической обработкой персональных данных. ФЗ «О персональных данных» и «Об информации, информационных технологиях и защите информации» о порядке правовой защиты персональных данных. Глава 14 Трудового кодекса РФ как основа регулирования персональных данных работника. Персональные данные государственных служащих (4).	22
10 (13). Ответственность за нарушение информационного законодательства	8

Итого	**48**

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

Вид СРС	**Трудоемкость в часах**
	ОФ
Ознакомление с содержанием основной и дополнительной литературы, методических материалов, конспектов лекций для подготовки к занятиям	8
Оформление отчетов по практическим и(или) лабораторным работам	14
Подготовка к промежуточной аттестации	6
Итого	**28**

5 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине "Организационное и правовое обеспечение информационной безопасности"

5.1 Паспорт фонда оценочных средств

Планируемые результаты обучения по дисциплине (модулю)

Дисциплина направлена на формирование следующих компетенций выпускника:

Форма(ы) текущего контроля	**Компетенции, формируемые в результате освоения дисциплины (модуля)**	**Индикатор(ы) достижения компетенции**	**Результаты обучения по дисциплине (модулю)**	**Уровень**
Опрос по контрольным вопросам или тестирование, подготовка отчетов по практическим и(или) лабораторным работам	ОПК-5 - Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	Применяет нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	**Знать** основы российской правовой системы и законодательства, правового статуса личности, организации деятельности органов государственной власти Российский Федерации по защите информации; виды и степень ответственности за правонарушения и преступления в информационной сфере. **Уметь** применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; анализировать правовые акты и осуществлять правовую оценку информации. **Владеть** навыками поиска нормативной правовой информации. необходимой для профессиональной деятельности навыками работы с нормативными правовыми актами.	Высокий или средний

Опрос по контрольным вопросам или тестирование, подготовка отчетов по практическим и(или) лабораторным работам	ОПК-6 - Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Организует защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	**Знать** характеристику основных отраслей российского права, правовые основы обеспечения национальной безопасности РФ; основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации. **Уметь** определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; предпринимать необходимые меры по восстановлению нарушенных прав. **Владеть** навыками организации охраны объектов информатизации и обеспечения режима секретности, организации и управления деятельностью службы защиты информации на предприятии.	Высокий или средний
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** порядок работы с персоналом по вопросам обеспечения защиты информации ограниченного доступа, проведения мероприятий по физической и технической защите конфиденциальной информации, организации службы безопасности предприятия; правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях. **Уметь** разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации; организовывать работы по проверке кандидатов на должность, текущую работу с персоналом \ю обеспечению информационной безопасности. **Владеть** навыками работы с персоналом, принятия организационно-управленческих решений, в том числе в нестандартных ситуациях в целях обеспечения 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. 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. Организационное обеспечение информационной безопасности.

1. Кто принимает решение о допуске гражданина к сведениям, составляющим государственную тайну?
2. Кто допускается к государственной тайне в особом порядке (без проведения проверочных мероприятий)?
3. Какие задачи должен решать пропускной режим?
4. Кто утверждает пропускной и внутриобъектовый режим в учреждении?
5. Кто отвечает за правильную эксплуатацию и своевременный контроль за состоянием средств защиты, выданных в индивидуальное пользование?

2. Правовое обеспечение информационной безопасности.

1. Что является основным нормативно-правовым документом, защищающим права, свободы и безопасность человека в системе информационных отношений, в РФ?

2. Какая информация относится к государственной тайне?
3. Каким нормативным документом введена защита компьютерной информации?
4. Какие сведения составляют Государственную тайну ?
5. Какие существуют режимы доступа к конфиденциальной информации?

Примерный перечень тестовых заданий:

1. Организационное обеспечение информационной безопасности.

1. Кто принимает решение о допуске гражданина к сведениям, составляющим государственную тайну?

руководитель территориальных органов исполнительной власти, наделенных полномочиями по защите государственной тайны
руководитель предприятия, на котором работает гражданин
руководитель органа ФСБ, проводившего проверочные мероприятия

2. Работники охраны предприятия имеют право требовать от персонала и посетителей объектов охраны соблюдения внутриобъектового и пропускного режимов:

При обеспечении внутриобъектового и пропускного режимов, а также при транспортировке охраняемых грузов, денежных средств и иного имущества в пределах объекта охраны
При осуществлении обязанностей по защите жизни и здоровья граждан
При обеспечении любых охранных мероприятий, предусмотренных законодательством

3. Какие работники относятся к оперативному персоналу?

Работники, специально обученные и подготовленные для оперативного обслуживания в утвержденном объеме закрепленных за ним оборудования
Работники, выполняющие техническое обслуживание и ремонт, монтаж, наладку и испытание оборудования
Работники, на которых возложены обязанности по организации технического и оперативного обслуживания, проведения ремонтных, монтажных и наладочных работ с оборудованием
нет верного ответа

2. Правовое обеспечение информационной безопасности

1. Основным нормативно-правовым документом, защищающим права, свободы и безопасность человека в системе информационных отношений, в РФ является:

Стратегия национальной безопасности РФ до 2020 года
ФЗ "О государственной тайне"
Конституция
Уголовный кодекс
Доктрина информационной безопасности РФ

2. Какие режимы доступа к конфиденциальной информации существуют: (выбрать все верные)

общественного достояния
исключительных прав
массовой информации
конфиденциальной информации
свободного доступа
неограниченного доступа

3. Преступлениям в сфере компьютерной информации в Уголовном кодексе посвящается

глава
раздел
статья
пункт
часть

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 является зачет, 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 зачете 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 зачет:

1. Угрозы безопасности информации.
2. Система защиты информации.
3. Законодательно - правовые и организационные основы обеспечения защиты информации.
4. Организация защиты информации на предприятии.
5. Политика безопасности предприятия.
6. Структура системы государственного лицензирования.
7. Порядок проведения лицензирования.
8. Основные лицензионные требования и условия.
9. Порядок проведения аттестации и контроля объектов информатизации.
10. Объекты защиты.

11. Структура системы сертификации.
12. Перечень видов деятельности в области защиты информации, подлежащих лицензированию.
13. Государственная аттестация руководителей предприятий.
14. Организационные и технические способы защиты государственной тайны.
15. Организационное управление защитой информации.
16. Перечень сведений конфиденциального характера.
17. Мероприятия по защите конфиденциальной информации.
18. Законодательство РФ о ГТ. Полномочия органов государственной власти и должностных лиц.
19. Перечень сведений, составляющих ГТ. Отнесение сведений к ГТ.
20. Порядок засекречивания сведений и их носителей.
21. Порядок рассекречивания сведений и их носителей.
22. Распоряжение сведениями, составляющими ГТ.
23. Органы защиты ГТ.
24. Порядок допуска к ГТ.
25. Контроль за обеспечением защиты государственной тайны.
26. Правила отнесения сведений, составляющих ГТ, к различным степеням секретности.
27. Организация допуска должностных лиц и граждан к государственной тайне.
28. Информация как объект правового регулирования.
29. Виды информации, защищаемой законодательством РФ.
30. Государственная тайна как особый вид защищаемой информации.
31. Система защиты государственной тайны.
32. Организационное управление защитой информации. (Принципы ИБ предприятия. Направления (методическое, организационной, техническое) и этапы по созданию комплексной системы безопасности. Уровни ПБ предприятия.)
33. Структура организационной защиты информации. (Объекты защиты. Структура организации защиты информации (СЗИ; мероприятия по ЗИ; мероприятия по контролю эффективности защиты информации.)
34. Организация и порядок проведения специальных экспертиз предприятий.
35. Порядок оформления запроса на лицензирование по видам деятельности.
36. Порядок отнесения сведений к коммерческой тайне. (Закон о КТ).
37. Информация, которая не подлежит засекречиванию.
38. Обеспечение сохранности документов, дел и изданий.
39. Обязанности лиц, допущенных к сведениям, составляющих коммерческую тайну.
40. Организация контроля за обеспечением режима при работе со сведениями, содержащими коммерческую тайну.
41. Обязанности персонала организации по сохранению коммерческой тайны.
42. Состав и структура системы безопасности предприятия.
43. Правовые основы деятельности службы безопасности.
44. Организационное обеспечение информационной безопасности при проведении закрытых мероприятий.
45. Организация информационно - аналитической работы.
46. Организация охраны предприятий.
47. Основные задачи организации режима и охраны.
48. Организация пропускного режима.
49. Пропускные документы.
50. Требования внутриобъектового режима.
51. Основные документы, разрабатываемые на охраняемых объектах.
52. Организация информационной безопасности и защиты информации.

Примерный перечень тестовых заданий на зачет:

1. Кто принимает решение о допуске гражданина к сведениям, составляющим государственную тайну?

руководитель территориальных органов исполнительной власти, наделенных полномочиями по защите государственной тайны
руководитель предприятия, на котором работает гражданин
руководитель органа ФСБ, проводившего проверочные мероприятия

2. Работники охраны предприятия имеют право требовать от персонала и посетителей объектов

охраны соблюдения внутриобъектового и пропускного режимов:

При обеспечении внутриобъектового и пропускного режимов, а также при транспортировке охраняемых грузов, денежных средств и иного имущества в пределах объекта охраны
При осуществлении обязанностей по защите жизни и здоровья граждан
При обеспечении любых охранных мероприятий, предусмотренных законодательством

3. Какие работники относятся к оперативному персоналу?

Работники, специально обученные и подготовленные для оперативного обслуживания в утвержденном объеме закрепленных за ним оборудования
Работники, выполняющие техническое обслуживание и ремонт, монтаж, наладку и испытание оборудования
Работники, на которых возложены обязанности по организации технического и оперативного обслуживания, проведения ремонтных, монтажных и наладочных работ с оборудованием
нет верного ответа

4. Основным нормативно-правовым документом, защищающим права, свободы и безопасность человека в системе информационных отношений, в РФ является:

Стратегия национальной безопасности РФ до 2020 года
ФЗ "О государственной тайне"
Конституция
Уголовный кодекс
Доктрина информационной безопасности РФ

5. Какие режимы доступа к конфиденциальной информации существуют: (выбрать все верные)

общественного достояния
исключительных прав
массовой информации
конфиденциальной информации
свободного доступа
неограниченного доступа

6. Преступлениям в сфере компьютерной информации в Уголовном кодексе посвящается

глава
раздел
статья
пункт
часть

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. 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: 16.04.2026). – Библиогр. в кн. – Текст : электронный.

2. 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: 23.03.2026). — Режим доступа: для авториз. пользователей.

3. Мальцев, В. А. Правовое обеспечение информационной безопасности в российской федерации : учебно-методическое пособие / В. А. Мальцев. — Воронеж : ВГУ, 2017. — 40 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/154824 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

4. Белов, Е. Б. Организационно-правовое обеспечение информационной безопасности : учебник для студентов учреждений среднего профессионального образования / Е. Б. Белов, В. Н. Пржегорлинский ; Е. Б. Белов, В. Н. Пржегорлинский. – 3-е изд., стер. – Москва : Академия, 2021. – 336 с. с. – (Профессиональное образование). – URL: https://academia-moscow.ru/reader/?id=711770 (дата обращения: 23.03.2026). – Текст : электронный.

5. Прокопенко, Е. В. Категорирование объектов критической информационной инфраструктуры : учебное пособие для студентов, обучающихся по образовательным программам высшего образования и среднего профессионального образования по специальностям и направлениям подготовки, входящим в укрупненную группу специальностей и направлений подготовки 10.00.00 "Информационная безопасность" / Е. В. Прокопенко, В. О. Коротин ; Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, 2025. – 1 файл (1,03 Мб). – URL: http://library.kuzstu.ru/meto.php?n=92010&type=utchposob:common (дата обращения: 23.03.2026). – Текст : электронный.

6.2 Дополнительная литература

1. Ажмухамедов, И. М. Основы организационно-правового обеспечения информационной безопасности : учебное пособие : [16+] / И. М. Ажмухамедов, О. М. Князева. – Санкт-Петербург : Интермедия, 2017. – 264 с. : табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=481107 (дата обращения: 11.04.2026). – Библиогр.: с. 248-256. – ISBN 978-5-4383-0160-8. – 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: 23.03.2026). — Режим доступа: для авториз. пользователей.

6.3 Методическая литература

1. Организационное и правовое обеспечение информационной безопасности : 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. – Ч. 1: Организационное обеспечение информационной безопасности. – Кемерово : КузГТУ, 2018. – 45 с. – URL: http://library.kuzstu.ru/meto.php?n=9102 (дата обращения: 23.03.2026). – 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. Научная электронная библиотека eLIBRARY.RU https://elibrary.ru/projects/subscription/rus_titles_open.asp?
7. Национальная электронная библиотека https://rusneb.ru/

6.5 Периодические издания

1. Безопасность информационных технологий: научный журнал

https://eivis.ru/browse/publication/379646

2. Защита информации. Инсайд: информационно-методический журнал https://eivis.ru/browse/publication/122426

3. 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 "Организационное и правовое обеспечение 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 "Организационное и правовое обеспечение 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. 7-zip
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 "Организационное и правовое обеспечение информационной безопасности"

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.