

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 16:00:31

Дубинкин Дмитрий Михайлович

Рабочая программа дисциплины

Управление информационной безопасностью

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.



1784257142

Рабочую программу составил:

ПОДПИСАНО ЭП КУЗГТУ

Подразделение: кафедра информационной безопасности

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

Дата: 17.07.2026 09:59:29

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 09:59:50

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 10:00:09

Прокопенко Евгения Викторовна



1784257142

1 Перечень планируемых результатов обучения по дисциплине "Управление информационной безопасностью", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:
обще профессиональных компетенций:

ОПК-1 - Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;

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

Результаты обучения по дисциплине определяются индикаторами достижения компетенций

Индикатор(ы) достижения:

Обосновывает требования к системе обеспечения информационной безопасности и разрабатывает проекты технического задания на ее создание.

Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности

Результаты обучения по дисциплине:

Знать основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; основные механизмы информационной безопасности и типовые процессы управления этими механизмами в информационной системе; основные угрозы безопасности информации и модели нарушителя в информационных системах; принципы формирования политики информационной безопасности в информационных системах; методы аттестации уровня защищенности информационных систем; основные методы управления информационной безопасностью; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем.

Знает нормативную и правовую базу в области управления информационной безопасностью объектов критической информационной инфраструктуры. Знает отечественные и зарубежные стандарты в области управления информационной безопасностью объектов критической информационной инфраструктуры. Знает структуру политик обеспечения информационной безопасности объектов критической информационной инфраструктуры и требования к их содержанию

Уметь строить системы обеспечения информационной безопасности в различных условиях функционирования защищаемых информационных систем; разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; разрабатывать частные политики информационной безопасности информационных систем; контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем; оценивать информационные риски в информационных системах; разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем; составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности.

Умеет разрабатывать проекты нормативных и организационно-распорядительных документов по обеспечению информационной безопасности объектов критической информационной инфраструктуры. Умеет разрабатывать политику информационной безопасности объектов критической информационной инфраструктуры различных уровней

Владеть методами и средствами выявления угроз безопасности информационным системам; навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем; навыками участия в экспертизе состояния защищенности информации на объекте защиты; методами управления информационной безопасностью информационных систем; методами оценки информационных рисков; методами организации и управления деятельностью служб защиты информации на предприятии; навыками управления информационной безопасностью простых объектов.

Владеет навыками разработки политики информационной безопасности различных уровней

2 Место дисциплины "Управление информационной безопасностью" в структуре ОПОП магистратуры

Для освоения дисциплины необходимо владеть знаниями умениями, навыками, полученными в



1784257142

рамках высшего образования и (или) дополнительного профессионального образования.

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 "Управление информационной безопасностью" в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся

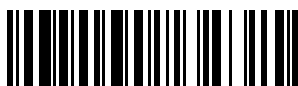
Общая трудоемкость дисциплины "Управление информационной безопасностью" составляет 7 зачетных единиц, 252 часа.

Форма обучения	Количество часов		
	ОФ	ЗФ	ОЗФ
Курс 1/Семестр 1			
Всего часов			252
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			120
Самостоятельная работа			72
Форма промежуточной аттестации			экзамен /36

4 Содержание дисциплины "Управление информационной безопасностью", структурированное по разделам (темам)

4.1. Лекционные занятия

Раздел дисциплины, темы лекций и их содержание	Трудоемкость в часах	
	ОФ	ОЗФ
1 ОСНОВНЫЕ ПОНЯТИЯ И ПОДХОДЫ К УПРАВЛЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ • Сущность информационной безопасности, ее составляющие • Нормативно-правовые аспекты и методы регулирования в области информационной безопасности • Система управления информационной безопасностью • Политика информационной безопасности	2	2
2 ОСНОВНЫЕ КРИТЕРИИ ВЫБОРА СРЕДСТВ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ НА ПРЕДПРИЯТИИ • Перечень защищаемой информации на предприятии • Формирование матрицы и модели доступа к управлению информационной безопасностью • Основные виды угроз информационной безопасности • Модель нарушителя информационной безопасности	2	2



1784257142

3. МЕРОПРИЯТИЯ ПО УПРАВЛЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ НА ПРЕДПРИЯТИИ • Определение режима управления информацией на предприятии • Разработка подсистемы управления доступом защищаемой информации • Контроль за работой средствами управления информационной безопасностью (СУИБ) на предприятии • Мониторинг и оценка рисков управления информационной безопасностью	4	4
4. ПРАКТИЧЕСКИЕ АСПЕКТЫ СОЗДАНИЯ СУИБ • Политика информационной безопасности • Угрозы информационной безопасности. Построение модели угроз • Причинно-следственный анализ угроз и уязвимостей в системе управления информационной безопасностью предприятия • Документированные процедуры УИБ • Оценка информационных рисков на основе причинно-следственных связей угроз и уязвимостей • Положение о применимости результатов в СУИБ	4	4
Итого	12	12

4.2 Практические (семинарские) занятия

Тема занятия	Трудоемкость в часах	
	ОФ	ОЗФ
№ 1 МЕНЕДЖМЕНТ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	2	2
№ 2 МЕЖДУНАРОДНЫЕ ОРГАНИЗАЦИИ В СФЕРЕ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	1	1
№ 3 МЕНЕДЖМЕНТ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ГОСУДАРСТВЕННОМ УРОВНЕ В РФ	1	1
№ 4 ИЗУЧЕНИЕ СТАНДАРТА ГОСТ Р ИСО/МЭК 27001-2021	2	2
№ 5 ОСНОВНЫЕ ЭТАПЫ СОЗДАНИЯ СУИБ. АНАЛИЗ РИСКОВ	2	2
№ 6 ОСНОВНЫЕ ЭТАПЫ СОЗДАНИЯ СУИБ. РАЗРАБОТКА ПОЛИТИК И ПРОЦЕДУР.	2	2
№ 7 ОЦЕНКА ИНФОРМАЦИОННЫХ РИСКОВ ОРГАНИЗАЦИЙ С ИСПОЛЬЗОВАНИЕМ MICROSOFT SECURITY ASSESSMENT TOOL	2	2
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	30	30
Оформление отчетов по практическим и(или) лабораторным работам	36	36



1784257142

Подготовка к промежуточной аттестации	6	6
Итого	72	72
Самостоятельная работа под руководством преподавателя	120	120
Экзамен	36	36

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 "Управление информационной безопасностью"

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) текущего контроля	Компетенции, формируемые в результате освоения дисциплины (модуля)	Индикатор(ы) достижения компетенции	Результаты обучения по дисциплине (модулю)	Уровень



1784257142

Опрос по контрольным вопросам, подготовка отчетов по практическим и (или) лабораторным работам	ОПК-1	Обосновывает требования к системе обеспечения информационной безопасности и разрабатывает проекты технического задания на ее создание	Знать основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; основные механизмы информационной безопасности и типовые процессы управления этими механизмами в информационной системе; основные угрозы безопасности информации и модели нарушителя в информационных системах; принципы формирования политики информационной безопасности в информационных системах; методы аттестации уровня защищенности информационных систем; основные методы управления информационной безопасностью; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем. Уметь строить системы обеспечения информационной безопасности в различных условиях функционирования защищаемых информационных систем; разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; разрабатывать частные политики информационной безопасности информационных систем; контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем; оценивать информационные риски в информационных системах; разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем; составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности. Владеть методами и средствами выявления угроз безопасности информационным системам; навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем; навыками участия в экспертизе состояния защищенности информации на объекте защиты; методами управления информационной безопасностью информационных систем; методами оценки информационных рисков; методами организации и управления деятельностью служб защиты информации на предприятии; навыками управления информационной безопасностью простых объектов.	Высокий или средний
--	-------	---	---	---------------------



1784257142

Опрос по контрольным вопросам, подготовка отчетов по практическим (или) лабораторным работам	ОПК-3	Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	Знает нормативную и правовую базу в области управления информационной безопасностью объектов критической информационной инфраструктуры. Знает отечественные и зарубежные стандарты в области управления информационной безопасностью объектов критической информационной инфраструктуры. Знает структуру политик обеспечения информационной безопасности объектов критической информационной инфраструктуры и требования к их содержанию. Умеет разрабатывать проекты нормативных и организационно-распорядительных документов по обеспечению информационной безопасности объектов критической информационной инфраструктуры. Умеет разрабатывать политику информационной безопасности объектов критической информационной инфраструктуры различных уровней. Владеет навыками разработки политики информационной безопасности различных уровней	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, оформлении отчетов по лабораторным работам.

Опросе обучающихся по контрольным вопросам

Обучающийся отвечает на 2 вопроса.

Например:

ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;

Содержание вопроса (задания)	Правильный ответ
Основной процесс управления ИБ, результатом которого является перечень недопустимых последствий и обоснование необходимости внедрения конкретных мер защиты в ТЗ, называется оценка _____.	рисков
Высокоуровневый документ организации, на основе которого формулируются общие требования к проектируемой системе защиты и определяются цели обеспечения безопасности, называется _____ информационной безопасности.	политика

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

Содержание вопроса (задания)	Правильный ответ
Совокупность документов, регламентирующих вопросы защиты информации и изданных руководством организации в рамках своей компетенции, составляет организационно-_____ документацию по ИБ.	распорядительную
При разработке проекта документа, устанавливающего запрет на разглашение коммерческой тайны, обязательным приложением к трудовому договору является _____ о неразглашении.	Обязательство



1784257142

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

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.

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:

ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;



1784257142

Содержание вопроса (задания)	Правильный ответ
Основной процесс управления ИБ, результатом которого является перечень недопустимых последствий и обоснование необходимости внедрения конкретных мер защиты в ТЗ, называется оценка _____.	рисков
Высокоуровневый документ организации, на основе которого формулируются общие требования к проектируемой системе защиты и определяются цели обеспечения безопасности, называется _____ информационной безопасности.	политика

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

Содержание вопроса (задания)	Правильный ответ
Совокупность документов, регламентирующих вопросы защиты информации и изданных руководством организации в рамках своей компетенции, составляет организационно-_____ документацию по ИБ.	распорядительную
При разработке проекта документа, устанавливающего запрет на разглашение коммерческой тайны, обязательным приложением к трудовому договору является _____ о неразглашении.	Обязательство
Реквизит документа, содержащий дату, регистрационный номер и место составления, называется _____ данными документа.	справочными
Документ, определяющий задачи, функции, права и ответственность подразделения (отдела), отвечающего за защиту информации в компании, называется _____ об отделе ИБ.	Положение

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-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;

Содержание вопроса (задания)	Правильный ответ
Какой процесс в управлении ИБ является первичным для обоснования выбора мер защиты и формирования требований в техническом задании? 1. Закупка оборудования. 2. Оценка рисков информационной безопасности. 3. Написание должностных инструкций. 4. Проведение инвентаризации мебели в офисе.	2
При разработке ТЗ требование к «минимизации прав доступа», когда пользователю предоставляются только те полномочия, которые необходимы для выполнения работы, обосновывается принципом: 1. Максимальной открытости. 2. Производственной необходимости (наименьших привилегий). 3. Удобства администрирования. 4. Экономии оперативной памяти.	2



1784257142

Содержание вопроса (задания)		Правильный ответ
Установите соответствие методов обработки рисков и проектных решений в ТЗ		А - 2, Б - 3, В - 1.
Метод обработки риска	Техническое/организационное решение в ТЗ	
А) Снижение (минимизация)	1) Отказ от использования облачных сервисов для хранения гостайны	
Б) Передача (перекладывание)	2) Внедрение системы двухфакторной аутентификации и шифрования	
В) Уклонение (избегание)	3) Заключение договора страхования киберрисков или аутсорсинг ИБ	
Установите соответствие документов по управлению ИБ и их роли при разработке ТЗ		А - 2, Б - 1, В - 3.
Документ	Роль в обосновании требований	
А) Политика ИБ	1) Описание конкретных векторов атак для выбора средств защиты	
Б) Модель угроз	2) Фундамент, определяющие общие принципы и цели защиты	
В) Техническое задание	3) Детальный перечень требований к реализации системы защиты	
Установите правильную последовательность этапов управления рисками для обоснования требований к системе защиты: 1. Выбор мер и средств защиты для нейтрализации угроз. 2. Идентификация информационных активов и их ценности. 3. Анализ и оценка вероятности реализации угроз. 4. Определение остаточного риска после внедрения мер.		2, 3, 1, 4.
Расставьте уровни нормативного обоснования требований к системе ИБ в порядке убывания их приоритетности (от общегосударственных к локальным): 1. Корпоративные инструкции и регламенты организации. 2. Федеральные законы и указы Президента РФ. 3. Отраслевые стандарты и требования регуляторов (ФСТЭК/ФСБ). 4. Политика информационной безопасности предприятия.		2, 3, 4, 1.

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

Содержание вопроса (задания)		Правильный ответ
Какой локальный нормативный акт является документом верхнего уровня в системе управления ИБ и служит базой для разработки всех остальных организационно-распорядительных документов? 1. 1. Инструкция по антивирусной защите. 2. 2. Политика информационной безопасности. 3. 3. Журнал учета машинных носителей. 4. 4. Приказ о назначении системного администратора.		2
Каким распорядительным документом в организации официально вводится в действие проект разработанного «Положения о защите персональных данных»? 1. 1. Служебной запиской. 2. 2. Приказом руководителя. 3. 3. Протоколом совещания. 4. 4. Трудовым договором.		2
Установите соответствие распорядительных документов и их целей в управлении ИБ		А - 2, Б - 3, В - 1.
Вид документа	Цель разработки документа	
А) Приказ	1) Описание детального порядка действий при инцидентах	
Б) Положение	2) Назначение ответственных лиц и ввод документов в действие	
В) Регламент	3) Определение структуры и функций подразделения защиты	



1784257142

Содержание вопроса (задания)		Правильный ответ
Установите соответствие реквизитов документа ИБ и их назначения (по ГОСТ)		А - 2, Б - 1, В - 3.
Реквизит	Значение для управления документом	
А) Гриф утверждения	1) Подтверждение согласия должностного лица с проектом	
Б) Виза согласования	2) Придание документу официальной юридической силы	
В) Гриф секретности	3) Определение правил обращения с носителем информации	
Расположите типы документов по информационной безопасности в порядке убывания их приоритетности в иерархии системы управления ИБ (СУИБ): 1. 1. Регламент проведения антивирусных проверок. 2. 2. Федеральное законодательство в области ИБ. 3. 3. Политика информационной безопасности организации. 4. 4. Должностная инструкция администратора ИБ.		2, 3, 1, 4.
Установите последовательность действий при подготовке проекта приказа о назначении ответственных за защиту персональных данных: 1. 1. Визирование проекта приказа у юриста и начальника отдела кадров. 2. 2. Определение круга должностных лиц, которые будут обрабатывать данные. 3. 3. Регистрация подписанного приказа и присвоение ему номера. 4. 4. Составление текста приказа с указанием конкретных обязанностей лиц.		2, 4, 1, 3.

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



1784257142

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 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. Капгер, И. В. Управление информационной безопасностью : учебное пособие / И. В. Капгер, А. С. Шабуров. — Пермь : ПНИПУ, 2023. — 91 с. — ISBN 978-5-398-02866-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/328889> (дата обращения: 28.03.2025). — Режим доступа: для авториз. пользователей.

2. Зырянова, Т. Ю. Управление информационной безопасностью : учебное пособие / Т. Ю. Зырянова. — Екатеринбург : , 2023. — 96 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/369482> (дата обращения: 28.03.2025). — Режим доступа: для авториз. пользователей.

3. Давыдов, А. И. Управление информационной безопасностью : учебное пособие / А. И. Давыдов, Д. А. Елизаров. — Омск : ОмГУПС, 2023. — 91 с. — ISBN 978-5-949-41321-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/419255> (дата обращения: 28.03.2025). — Режим доступа: для авториз. пользователей.

4. Милославская, Н. Г. Управление информационной безопасностью: Конспект лекций : учебное пособие / Н. Г. Милославская, А. И. Толстой. — Москва : НИЯУ МИФИ, 2020. — 536 с. — ISBN 978-5-7262-2694-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/284378> (дата обращения: 28.03.2025). — Режим доступа: для авториз. пользователей.

5. Дронова, Г. А. Управление информационной безопасностью : учебно-методическое пособие : [16+] / Г. А. Дронова. — Новосибирск : Новосибирский государственный технический университет, 2016. — 28 с. : ил., табл. — Режим доступа: по подписке. — URL: <https://biblioclub.ru/index.php?page=book&id=575356> (дата обращения: 10.09.2026). — Библиогр. в кн. —



1784257142

6.2 Дополнительная литература

1. Поздняк, И. С. Планирование и управление информационной безопасностью : учебное пособие / И. С. Поздняк, И. С. Макаров, Л. Р. Чупахина. — Самара : ПГУТИ, 2020. — 69 с. — ISBN 978-5-907336-42-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/411836> (дата обращения: 28.03.2025). — Режим доступа: для авториз. пользователей.

2. Поздняк, И. С. Планирование и управление информационной безопасностью : учебное пособие / И. С. Поздняк, И. С. Макаров, Л. Р. Чупахина. — Самара : ПГУТИ, 2020. — 69 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/255569> (дата обращения: 28.03.2025). — Режим доступа: для авториз. пользователей.

3. Поздняк, И. С. Управление информационной безопасностью : методические указания / И. С. Поздняк, И. С. Макаров. — Самара : ПГУТИ, 2019. — 43 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/223313> (дата обращения: 28.03.2025). — Режим доступа: для авториз. пользователей.

4. Золотарев, В. В. Управление информационной безопасностью. Ч. 1: Анализ информационных рисков : учебное пособие / В. В. Золотарев, Е. А. Данилова. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2010. - 144 с. - Текст : электронный. - URL: <https://znanium.com/catalog/product/463037> (дата обращения: 07.09.2026). - Режим доступа: по подписке.

5. Жукова, М. Н. Управление информационной безопасностью. Ч. 2: Управление инцидентами информационной безопасности : учебное пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - 100 с. - Текст : электронный. - URL: <https://znanium.com/catalog/product/463061> (дата обращения: 07.09.2026). - Режим доступа: по подписке.

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: 28.03.2025). – Текст : электронный.

6.4 Профессиональные базы данных и информационные справочные системы

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

6.5 Периодические издания

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

7 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

ЭИОС КузГТУ:

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



1784257142

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.

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 "Управление информационной безопасностью"

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 "Управление информационной безопасностью", включая перечень программного обеспечения и информационных справочных систем

Для изучения дисциплины может использоваться следующее программное обеспечение:

1. Mozilla Firefox
2. Yandex
3. GIMP
4. Open Office
5. Microsoft Windows
6. ESET NOD32 Smart Security Business Edition
7. Kaspersky Endpoint Security
8. Браузер Спутник

10 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине "Управление информационной безопасностью"

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

Перечень основного оборудования:

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

Моноблок (Intel Core i5-10400 / 8 Gb RAM); горизонт кабельный организатор (25B-1U-02BL);



1784257142

коммутац панель кат.5 (27B-U5-24BL 24 ports); коммутац панель кат.6 (27B-U6-24BL 24 ports); шкаф коммутац Eurolan (S3000-22U 600x600 мм, перед - стекло, зад - металл, 60F-22-66-31BL); коммутатор управляемый (D-Link DGS-3130-54TS 48 ports); программно-аппаратный комплекс (Infotecs IDS-1000); модуль доверенной загрузки (&amp;amp;amp;quot;Соболь-4&amp;amp;amp;amp;quot;); средство активной защиты информации от утечки за счет наводок информ сигнала на цепи заземления и электропитания (&amp;amp;amp;amp;quot;Соната-PC3&amp;amp;amp;quot;); точка доступа Wi-fi двухдиапазонная (D-Link DWL-8620AP); патч-корды кат 5 (Eurolan); патч-корды кат 6 (Eurolan);

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

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

Специальное помещение для самостоятельной работы № 1211

Перечень основного оборудования:

специализированная мебель (столы и стулья);

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

проектор, экран настенный моторизованный.

Специальное помещение для самостоятельной работы № 3210

Перечень основного оборудования:

специализированная мебель (столы и стулья);

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

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. ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. М., 2009, 50 с.

[Электронный ресурс]: — Режим доступа: <http://protect.gost.ru/document.aspx?control=7&id=173886>

2. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. М., 2022, 28 с.

[Электронный ресурс]: — Режим доступа: <https://protect.gost.ru/document.aspx?control=7&id=242006>.

3. ГОСТ Р ИСО/МЭК 27002-2021. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. М., 2021, 74 с.

[Электронный ресурс]: — Режим доступа: <https://protect.gost.ru/document.aspx?control=7&id=240766>

4. ГОСТ Р ИСО/МЭК 27003-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации. М., 2021, 46 с.

[Электронный ресурс]: — Режим доступа: <https://protect.gost.ru/document.aspx?control=7&id=240709>.

5. ГОСТ Р ИСО/МЭК 27004-2021. Информационная технология. Методы и средства обеспечения



1784257142

безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание. М., 2021, 50 с. [Электронный ресурс]: — Режим доступа: <https://protect.gost.ru/document.aspx?control=7&amp;amp;amp;id=240761>.

6. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. М., 2011, 51 с. [Электронный ресурс]: — Режим доступа: <http://protect.gost.ru/document.aspx?control=7&amp;amp;amp;id=177398>

7. ГОСТ Р ИСО/МЭК 27006-2020. Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности. М., 2021, 42 с. [Электронный ресурс]: — Режим доступа: <https://protect.gost.ru/document.aspx?control=7&amp;amp;amp;id=238756>

8. ГОСТ Р ИСО/МЭК 27007-2014. Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности. [Электронный ресурс]: — Режим доступа: <http://protect.gost.ru/document.aspx?control=7&amp;amp;amp;id=187871>

9. ГОСТ Р ИСО/МЭК 27011-2012. Информационная технология. Методы и средства обеспечения безопасности. Руководства по менеджменту информационной безопасности для телекоммуникационных организаций на основе ИСО/МЭК 27002. [Электронный ресурс]: — Режим доступа: <http://protect.gost.ru/document.aspx?control=7&amp;amp;amp;id=183954>

10. ГОСТ Р ИСО/МЭК 27013-2014. Информационная технология. Методы и средства обеспечения безопасности. Руководство по совместному использованию стандартов ИСО/МЭК 27001 и ИСО/МЭК 20000-1. [Электронный ресурс]: — Режим доступа: <http://protect.gost.ru/document.aspx?control=7&amp;amp;amp;id=187948>

11. ГОСТ Р ИСО/МЭК 27031-2012. Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса. [Электронный ресурс]: — Режим доступа: <http://protect.gost.ru/document.aspx?control=7&amp;amp;amp;id=184904>

12. ГОСТ Р ИСО/МЭК 27033-1-2011. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. [Электронный ресурс]: — Режим доступа: <http://protect.gost.ru/document.aspx?control=7&amp;amp;amp;id=179072>

13. ГОСТ Р ИСО/МЭК 27033-3-2011. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления. [Электронный ресурс]: — Режим доступа: <http://protect.gost.ru/document.aspx?control=7&amp;amp;amp;id=187869>

14. ГОСТ Р ИСО/МЭК 27034-1-2014. Информационная технология. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 1. Обзор и общие понятия. [Электронный ресурс]: — Режим доступа: <http://protect.gost.ru/document.aspx?control=7&amp;amp;amp;id=187929>

15. ГОСТ Р ИСО/МЭК 27037-2014. Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме. [Электронный ресурс]: — Режим доступа: <http://protect.gost.ru/document.aspx?control=7&amp;amp;amp;id=187854>

16. ГОСТ Р ИСО/МЭК 27038-2016. Информационные технологии. Методы обеспечения безопасности. Требования и методы электронного цензурирования. [Электронный ресурс]: — Режим доступа: <http://protect.gost.ru/document1.aspx?control=31&amp;amp;amp;id=204467>

17. 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. [Электронный ресурс]: — Режим доступа: <https://e.lanbook.com/book/167600>.



1784257142