МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«КЕМЕРОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Кузбасский гуманитарно-педагогический институт

Факультет информатики, математики и экономики

УТВЕРЖДАЮ
Декан
Фомина А.В.
«16» января 2025_ г.

Рабочая программа дисциплины

К.М.07.01.12 Информационная безопасность

Направление подготовки
44.03.04 Профессиональное обучение (по отраслям)

Направленность (профиль)
Аддитивные технологии

Программа бакалавриата

Квалификация выпускника
бакалавр

Форма обучения
заочная

Год набора 2025

Новокузнецк 2025

Оглавление

1 Цель дисциплины.

В результате освоения дисциплины у обучающегося должны быть сформированы компетенции основной профессиональной образовательной программы бакалавриата (далее - ОПОП):

ПК – 1

Формируемые компетенции, индикаторы достижения компетенций, знания, умения, навыки

Таблица 1 – Индикаторы достижения компетенций, формируемые дисциплиной

Код и название компетенции	Индикаторы достижения компетенции по ОПОП	Знания, умения, навыки (ЗУВ), формируемые дисциплиной
ПК – 1 Способен осваивать и использовать теоретические знания и практические умения и навыки в предметной области по профилю "Аддитивные технологии" при решении профессиональных задач	ПК 1.1 Демонстрирует владение методами работы над объектами визуальной информации, владение композиционными приемами и стилистическими особенностями проектируемого объекта визуальной информации ПК 1.2 Демонстрирует методы использования программных и аппаратных средств для создания 3D-моделей	Знать: - виды и источники угроз безопасности информации; - основные требования информационной безопасности; - основные элементы информационной поддержки решения задачи защиты информации Уметь: - выбирать методы и разрабатывать средства защиты информации; Владеть: - навыками применения современных средств информационной безопасности - способами анализа и отбора методов и средств обеспечения информационной безопасности при работе в электронной среде обучения

2 Объём и трудоёмкость дисциплины по видам учебных занятий. Формы промежуточной аттестации.

Таблица 2 – Объем и трудоемкость дисциплины по видам учебных занятий

Общая трудоемкость и виды учебной работы по дисциплине, проводимые в разных формах	Объём часов по формам обучения		
	ОФО	ОЗФО	ЗФО
1 Общая трудоемкость дисциплины			180
2 Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)			
Аудиторная работа (всего):			
в том числе:			
лекции			6
практические занятия, семинары			
практикумы			10
лабораторные работы			
Внеаудиторная работа (всего):			
в том числе, индивидуальная работа обучающихся с преподавателем			
подготовка курсовой работы (проекта) /контактная работа			
групповая, индивидуальная консультация и иные виды			

учебной деятельности, предусматривающие групповую или индивидуальную работу обучающихся с преподавателем*)*			
творческая работа (эссе)			
3 Самостоятельная работа обучающихся (всего)			160
4 Промежуточная аттестация обучающегося - и объём часов, выделенный на промежуточную аттестацию:			4 ЗаО 5 з.е.

3. Учебно-тематический план и содержание дисциплины.

3.1 Учебно-тематический план

Таблица 3 - Учебно-тематический план заочной формы обучения

№ недели п/п	Разделы и темы дисциплины по занятиям	Общая трудоёмкость *(всего час.)*	Трудоемкость занятий (час.)									Формы текущ. контроля и промежуточной аттестации
			ОФО			ОЗФО			ЗФО			
			Аудиторн. занятия		СРС	Аудиторн. занятия		СРС	Аудиторн. занятия		СРС	
			лекц.	практ		лекц.	практ		лекц.	практ		
Семестр ___4___												
1.	**Раздел 1. Основы информационной безопасности**											
1	1.1 Основные понятия ИБ.	26							2	2	22	
2	1.2 Уровни обеспечения ИБ	24								2	22	
2.	**Раздел 2.Основные подходы к обеспечению информационной безопасности образовательной организации**											
3	2.1 Типовые информационные процессы ОО, оценка рисков и принципы защиты информации	24							2		22	
4	2.2 Политика информационной безопасности ОО	24							2		22	
5	2.3 Механизмы и средства сетевой безопасности	26								2	24	
6	2.4 Криптографические средства защиты информации, электронная цифровая подпись	26								2	24	
7	2.5 Средства фильтрации Интернет-контента	26								2	24	
8	Промежуточная аттестация - зачет с оценкой	4										ЗаО
9	Всего по учебному плану:	180							6	10	160	4

4 Порядок оценивания успеваемости и сформированности компетенций обучающегося в текущей и промежуточной аттестации.

Для положительной оценки по результатам освоения дисциплины обучающемуся необходимо выполнить все установленные виды учебной работы. Оценка результатов работы обучающегося в баллах (по видам) приведена в таблице 4.

Таблица 4 - Балльно-рейтинговая оценка результатов учебной работы обучающихся по видам (БРС)

Учебная работа (виды)	Сумма баллов	Виды и результаты учебной работы	Оценка в аттестации	Баллы за освоение дисциплины (мин.-макс.)

Текущая учебная работа в семестре (Посещение занятий по расписанию и выполнение заданий)	**80**	Лабораторные работы (отчет о выполнении лабораторной работы) (5 занятий).	10 баллов - посещение 1 пр. занятия и выполнение задания на 51-65% 20 баллов – посещение 1 пр. занятия и выполнение задания на 85-100%, самостоятельность и существенный вклад на занятии в работу группы, др.	0-40
		Самостоятельная работа	20 б - выполнение задания на 51-65% 40 б - выполнение задания на 85-100%	0-40
Итого по текущей работе в семестре				**0-80**
Промежуточная аттестация (зачет)	**20**	Теоретический вопрос	5 баллов (пороговое значение) 10 баллов (максимальное значение)	5 - 10
		Выполнение задания	5 баллов (пороговое значение) 10 баллов (максимальное значение)	5 - 10
Итого по промежуточной аттестации (зачету) по приведенной шкале (20б.)				0 – 20 б. (51 – 100%)
Суммарная оценка по дисциплине/ Сумма баллов текущей и промежуточной аттестации				**51 – 100 б.**

Обучающемуся по ЗФО задание на самостоятельную работу и контрольную работу выдается на установочной сессии.

5 Материально-техническое, программное и учебно-методическое обеспечение дисциплины.

5.1 Учебная литература

Основная учебная литература

1. Башлы П. Н. Информационная безопасность и защита информации: Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. ISBN 978-5-369-01178-2. – Текст : электронный // Знаниум : электронно-библиотечная система. - URL: http://znanium.com/catalog.php?bookinfo=405000 (дата обращения 24.05.20225). – Режим доступа : для авториз. пользователей.
2. Шаньгин В. Ф. Информационная безопасность. – М.: ДМК Пресс, 2014. – 702 с.: ил. ISBN 978-5-94074-768-0. – Текст : электронный // Лань : электронно-библиотечная система. - URL: http://e.lanbook.com/books/element.php?pl1_id=50578 (дата обращения 24.05.2025). – Режим доступа : для авториз. пользователей.

Дополнительная учебная литература

1. Бабаш А. В. Криптографические методы защиты информации. Том 3: Учебно-методическое пособие. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 216 с. ISBN 978- 5-369-01304-5. – Текст : электронный // Знаниум : электронно-библиотечная система. - URL: http://znanium.com/catalog.php?bookinfo=432654 (дата обращения 24.08.2019). – Режим доступа : для авториз. пользователей.
2. Баранова Е. К., Бабаш А. В. Моделирование системы защиты информации: Практикум: Учебное пособие. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015 - 120 с. ISBN 978-5- 369-01379-3. – Текст : электронный // Знаниум : электронно-библиотечная система. - URL: http://znanium.com/catalog.php?bookinfo=476047 (дата обращения 24.08.2019). – Режим доступа : для авториз. пользователей.

5.2 Материально-техническое и программное обеспечение дисциплины.

Учебные занятия по дисциплине проводятся в учебных аудиториях КГПИ КемГУ:

308 Компьютерный класс Учебная аудитория для проведения занятий лекционного типа,	654079, Кемеровская область, г. Новокузнецк, пр-кт Металлургов, д. 19

занятий лабораторного типа, для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации (мультимедийная) **Специализированная (учебная) мебель:** доска, кафедра, столы, стулья, **Оборудование для презентации учебного материала:** компьютер преподавателя, проектор, экран, 20 компьютеров **Лабораторное оборудование:** стационарное – компьютеры для обучающихся (20 шт.). **Используемое программное обеспечение:** Используемое программное обеспечение: Яндекс.Браузер (отечественное свободно распространяемое ПО), LibreOffice(свободно Распространяемое ПО), FoxitReader (свободно Распространяемое ПО), XAMPP (свободно распространяемое ПО), Denwer (свободно распространяемое ПО), MicrosoftVisualStudio Интернет с обеспечением доступа в ЭИОС	

5.3 Современные профессиональные базы данных и информационные справочные системы.

Перечень СПБД и ИСС по дисциплине

1. Федеральный портал «Российское образование» - http://www.edu.ru. Доступ свободный
2. Информационная система «Единое окно доступа к образовательным ресурсам» - http://www.window.edu.ru.
3. Федеральный центр информационно-образовательных ресурсов - http://fcior.edu.ru. Доступ свободный.
4. Федеральный портал "Информационно-коммуникационные технологии в образовании" - http://www.ict.edu.ru/.
5. Сайт Министерства образования и науки РФ. - Режим доступа: http://www.mon.gov.ru. Доступ свободный.
6. Единая коллекция цифровых образовательных ресурсов.- Режим доступа: http://school-collection.edu.ru/
7. Единое окно доступа к образовательным ресурсам. Раздел Образование в области техники и технологий – http://window.edu.ru/?p_rubr=2.2.75

6 Иные сведения и (или) материалы.

6.1.Примерные темы письменных учебных работ

6.1.1 Курсовая работа

6.1.2 Контрольные работы/ рефераты/ индивидуальные задания обучающемуся.

Задание для СРС

1. Вредоносное ПО: способы распространения, опасность, методы защиты.
2. Программные закладки: типы, способы внедрения и защиты.
3. Аппаратные средства защиты информации.
4. Сравнительный анализ средств защиты электронной почты.
5. Сравнительный анализ систем обнаружения атак.
6. Сравнительный анализ межсетевых экранов.
7. Анализ методов изучения поведения нарушителей безопасности компьютерных систем.

8. Анализ методов нарушения безопасности сетевых ОС и методов противодействия им.
9. Применение биометрической информации для аутентификации пользователей компьютерных систем.
10. Стандарты безопасности компьютерных систем и информационных технологий.
11. Сравнительный анализ методов и программных средств защиты от спама.
12. Методы и программные средства перехвата и анализа контента.
13. Уязвимости симметричных и асимметричных криптографических систем

6.2. Примерные вопросы и задания / задачи для промежуточной аттестации

Форма промежуточной аттестации экзамен.

Разделы и темы	Примерные теоретические вопросы	Примерные практические задания и (или) задачи
Семестр _5_ Зачет с оценкой		
Разделы дисциплины		
1. Основы информационной безопасности		
1.1 Основные понятия ИБ	1. Опишите основные угрозы целостности информации и способы противодействия им. 2. Опишите основные угрозы конфиденциальности информации и способы противодействия им.	Задача 1 (Анализ угроз) Ситуация: В компании используется общий файловый сервер, где сотрудники хранят рабочие документы. Недавно несколько файлов были случайно удалены, а в одном из них обнаружены несанкционированные изменения. Вопросы: Какие свойства ИБ были нарушены? Какие меры можно принять для предотвращения подобных ситуаций? Задача 2 (Разработка политики безопасности) Ситуация: Малое предприятие внедряет систему защиты данных, но не имеет четких правил. Задание: Составьте три базовых правила информационной безопасности для сотрудников (например, работа с паролями, использование USB-носителей, реагирование на подозрительные письма).
1.2 Уровни обеспечения ИБ	1. Укажите, к каким уровням ИБ относятся следующие средства: а) федеральный закон; б) антивирусное ПО; в) межсетевой экран; г) должностная инструкция сотрудника; д) распоряжение директора. 2. Каким образом необходимость защиты информации отражена в Конституции РФ?	Задача 1 (Правовой уровень) Ситуация: Компания разрабатывает мобильное приложение для обработки персональных данных пользователей. Руководство не уверено, какие законы и стандарты регулируют защиту данных в этом случае. Задание: Перечислите основные нормативные акты РФ, которые необходимо учитывать (например, ФЗ-152 «О персональных данных», ст. 13.11 КоАП). Какие требования GDPR (если приложение доступно в ЕС) могут применяться? Какие последствия возможны при нарушении этих норм? Цель: Определить правовые рамки и риски

		несоблюдения законодательства. Задача 2 (Организационный уровень) Ситуация: В организации нет четких инструкций по работе с конфиденциальной информацией. Сотрудники пересылают служебные документы через личную почту, используют слабые пароли и не блокируют компьютеры при уходе с рабочего места. Задание: Разработайте 3-4 пункта организационных мер для повышения ИБ (например, «Политика использования электронной почты», «Обязательная блокировка ПК при отсутствии»). Предложите метод контроля исполнения этих мер (например, аудит, обучение). Цель: Научиться формировать организационные меры защиты.
2. Основные подходы к обеспечению информационной безопасности образовательной организации		
2.1 Типовые информационные процессы ОО, оценка рисков и принципы защиты информации	1. Укажите три основные угрозы для информации в человеко-компьютерных системах. 2. Выделите три наиболее эффективных метода защиты информации от ошибочных действий пользователей.	1. Оценка рисков при внедрении облачного хранилища Контекст: Компания планирует перенести документооборот в облачный сервис (например, Яндекс.Диск или Google Drive). Задание: Проведите качественную оценку рисков (вероятность и последствия утечки, потери или блокировки данных). Сформулируйте 3-4 принципа защиты, которые необходимо учесть: Доступность (например, дублирование на локальный сервер) Конфиденциальность (шифрование, двухфакторная аутентификация) Соответствие законодательству (хранение данных в РФ для ФЗ-152). Какие организационные меры потребуются (инструкции для сотрудников, выбор ответственного за ИБ)? Цель: Отработать методику оценки рисков и выбора защитных мер для облачных решений.
2.2 Политика информационной безопасности ОО	1. Укажите основные требования к механизму авторизации пользователей в информационных системах организации.	1. Проанализируйте обоснованность положений предложенной политики ИБ, выработайте рекомендации по оптимизации Политики с учетом специфики организации.
2.3 Механизмыи средства сетевой безопасности	1. Укажите уровень эталонной модели OSI, в которые входит в функции шифрования.	1. Разработайте правила для сетевого фильтра, обеспечивающего работу протоколов Web, электронной почты, системы видеоконференций (по выбору) с учетом SSL-транспорта.

2.4 Криптографические средства защиты информации, электронная цифровая подпись	1. Опишите криптосистему, которая обладает Следующими чертами: предусматривает использование открытого ключа для шифрования и закрытого для дешифрования данных.	1. Предложите безопасный алгоритм восстановления забытого пароля электронной почты.
2.5 Средства фильтрации Интернет-контента	1. Сформулируйте цели и принципы контентной фильтрациив образовательной организации	1. Разработайте систему контент-фильтрации на основе открытых программных средств. Оцените ее надежность Для применения в образовательной организации.

Компетенции		
ПК – 1 Способен осваивать и использовать теоретические знания и практические умения и навыки в предметной области по профилю "Аддитивные технологии" при решении профессиональных задач		Кейс 1: Кража цифровой 3D-модели изделия Ситуация: На предприятии, занимающемся аддитивным производством, произошла утечка конфиденциальной 3D-модели нового изделия. Файл был похищен через взломанную учетную запись инженера, который использовал слабый пароль и не включил двухфакторную аутентификацию в системе управления проектами. Задачи: Какие технические меры (шифрование, контроль доступа, DLP) могли бы предотвратить утечку? Как организовать обучение сотрудников по кибергигиене (пароли, фишинг)? Какие юридические действия можно предпринять, если модель уже попала к конкурентам? Цель: Анализ уязвимостей в работе с цифровыми активами и разработка мер защиты.
		Кейс 2: Саботаж в производстве через вредоносный G-код Ситуация: На 3D-принтере было напечатано бракованное изделие из-за измененного G-кода. Расследование показало, что файл был подменен после передачи по незащищенному FTP-серверу. Подозревают действия злоумышленника или недобросовестного сотрудника. Задачи: Как обеспечить целостность и аутентичность управляющих файлов (G-код, STL)? Какие методы контроля доступа к оборудованию и ПО можно применить? Как внедрить систему журналирования изменений для отслеживания инцидентов? Цель: Понимание рисков подмены данных в аддитивном производстве и методов их минимизации.

Составитель (и): Читайло А.И., ассистент кафедры ИОТД
(*фамилия, инициалы и должность преподавателя (ей)*)