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
А.В. Фомина
«08» февраля 2024 г.

Рабочая программа дисциплины

К.М.08.01 Математические методы и программное обеспечение защиты информации

Направление подготовки
02.03.03 Математическое обеспечение и администрирование информационных систем

Направленность (профиль) подготовки
ПРОГРАММНОЕ И МАТЕМАТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Программа бакалавриата

Квалификация выпускника
бакалавр

Форма обучения
Очная

Год набора 2023

Новокузнецк 2024

Оглавление

1 Цель дисциплины.

В результате освоения данной дисциплины у обучающегося должны быть сформированы компетенции основной профессиональной образовательной программы бакалавриата (далее - ОПОП): ОПК-2, ОПК-3.

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
ОПК-2 Способен применять современный математический аппарат, связанный с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности	2.1 Решает задачу количественной оценки качества программного обеспечения 2.2 Применяет методы проектирования, разработки, и реализации программных продуктов 2.3 Использует инструментальные, программные и аппаратные средства измерений для оценки качества программного обеспечения	**Знать:** - основные виды криптографических методов и алгоритмов, принципы их построения и предъявляемые к ним требования принципы их построения и предъявляемые к ним требования. **Уметь**: - применять криптографические методы при проектировании и разработке программных продуктов. **Владеть**: - навыками использования основных видов криптографических алгоритмов при проектировании и разработке программных продуктов.
ОПК-3 Способен понимать и применять современные информационные технологии, в том числе отечественные, при создании программных продуктов и программных комплексов различного назначения	3.1 Применяет современные информационные технологии, в том числе отечественные, и инструментальные средства для производства программного продукта: 3.2 Использует современные информационные технологии для тестирования и отладки программного обеспечения; 3.3 Использует методы и средства автоматизации проектирования программных продуктов	**Знать:** - методы обеспечения информационной безопасности; - современные информационно-коммуникационные технологии; - основные требования к обеспечению информационной безопасности профессиональной деятельности в условиях цифровой экономики. **Уметь**: - применять методы защиты информации при создании программных продуктов. **Владеть**: - навыками обеспечения защиты информации в процессе создания программных продуктов.

Код и название компетенции	Индикаторы достижения компетенции по ОПОП	Знания, умения, навыки (ЗУВ), формируемые дисциплиной
	3.4 Владеет CASE (Computer-Aided Software Engineering) средствами 3.5 Анализирует и описывает принципы работы и требования к современным ИТ, ИС, СИИ, используемых в профессиональной деятельности в условиях цифровой экономики 3.6 Используем возможности современных ИТ, ИС, СИИ для решения типовых задач профессиональной деятельности	

Место дисциплины

Дисциплина включена в модуль «Современные информационные технологии» ОПОП ВО. Дисциплина осваивается на 3 курсе в 5 семестре.

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
1 Общая трудоемкость дисциплины	144
2 Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	42
Аудиторная работа (всего):	42
в том числе:	
лекции	6
лабораторные работы	36
в интерактивной форме	
3 Самостоятельная работа обучающихся (всего)	102
4 Промежуточная аттестация обучающегося – зачет с оценкой (5 семестр)	

3. Учебно-тематический план и содержание дисциплины.

3.1 Учебно-тематический план

Таблица 3 - Учебно-тематический план очной формы обучения

№ недели п/п	Разделы и темы дисциплины по занятиям	Общая трудоёмкость *(всего час.)*	Трудоемкость занятий (час.)			Формы текущего контроля и промежуточной аттестации успеваемости
			ОФО			
			Аудиторн. занятия		СРС	
			лекц.	лаб.		
Семестр 5						
	1. Информационная безопасность					Контрольная работа
1	1.1 Составляющие информационной безопасности	9,5	0,5	2	7	
2	1.2 Угрозы информационной безопасности	12,5	0,5	2	10	
3	1.3 Безопасность персональных данных	12		4	8	Защита отчета по ЛР №1,2
4	1.4 Каналы утечки и искажения информации	8		2	6	Защита отчета по ЛР №3
5	1.5 Нормативно-правовые основы информационной безопасности	10,5	0,5	4	6	
6	1.6 Информационная безопасность в компьютерных сетях	10,5	0,5	4	6	Защита отчета по ЛР №4,5
	2. Криптографические методы защиты информации					Контрольная работа
7	2.1 Основные понятия и история криптографии	8,5	0,5	2	6	Защита отчета по ЛР №6-7
8	2.2 Криптографические системы	14,5	0,5	2	12	Защита отчета по ЛР №8-10
9	2.3 Стеганография	13	1	2	10	Защита отчета по ЛР №11-13
10	2.4 Электронная цифровая подпись	10		2	8	Защита отчета по ЛР №14-15
	3. Механизмы обеспечения информационной безопасности					Контрольная работа
11	3.1 Контроль целостности информации	8,5	0,5	2	6	Защита отчета по ЛР №16
12	3.2 Идентификация и аутентификация	11,5	0,5	4	7	Защита отчета по ЛР №17-18
13	3.3 Методы разграничения доступа	15	1	4	10	
	Промежуточная аттестация					зачет
	Всего:	**144**	**6**	**36**	**102**	

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) в 5 семестре

Учебная работа (виды)	Сумма баллов	Виды и результаты учебной работы	Оценка в аттестации	Баллы
Текущая учебная работа в семестре (Посещение занятий по расписанию и выполнение заданий)	**60**	Посещение лекционных занятий (ведение конспекта) (9 лекций)	**0,6 баллов** - конспект 1 лекционного занятия	5
		Лабораторные работы (отчет о выполнении лабораторной работы) (18 работ).	**0,9 балла** - выполнение работы на 51-65% **1,2 балла** – выполнение работы на 65,1-100%	17 – 21

		Контрольные работы (3 работы)	**Контрольная работа по разделу** *1.* *Информационная безопасность* **Баллы за КР:** **6 баллов** (выполнено 51 - 65% заданий) **9 баллов** (выполнено 66 - 85% заданий) **11 баллов** (выполнено 86 - 100% заданий)	6-11
			Контрольная работа по разделу *2.* *Криптографические методы защиты информации* **Баллы за КР:** **7 баллов** (выполнено 51 - 65% заданий) **10 баллов** (выполнено 66 - 85% заданий) **12 баллов** (выполнено 86 - 100% заданий)	7-12
			Контрольная работа по разделу 3. *Механизмы обеспечения информационной безопасности* **Баллы за КР:** **6 баллов** (выполнено 51 - 65% заданий) **9 баллов** (выполнено 66 - 85% заданий) **11 баллов** (выполнено 86 - 100% заданий)	6-11
Итого по текущей работе в семестре				41 - 60
Промежуточная аттестация (экзамен)	40	Тест.	**6 балла** (пороговое значение) **10 баллов** (максимальное значение)	6 - 10
		Решение задачи 1.	**2 балла** (пороговое значение) **15 баллов** (максимальное значение)	2 - 15
		Решение задачи 2.	**2 балла** (пороговое значение) **15 баллов** (максимальное значение)	2 - 15
Итого по промежуточной аттестации (экзамену)				10 – 40 б.
Суммарная оценка по дисциплине: Сумма баллов текущей и промежуточной аттестации				51 – 100 б.

В промежуточной аттестации оценка выставляется в ведомость в 100-балльной шкале и в буквенном эквиваленте (таблица 5)

Таблица 5 – Соотнесение 100-балльной шкалы и буквенного эквивалента оценки

Сумма набранных баллов	Уровни освоения дисциплины и компетенций	*Экзамен*		*Зачет*
		Оценка	*Буквенный эквивалент*	*Буквенный эквивалент*
86 - 100	Продвинутый	5	отлично	Зачтено
66 - 85	Повышенный	4	хорошо	
51 - 65	Пороговый	3	удовлетворительно	
0 - 50	Первый	2	неудовлетворительно	Не зачтено

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

5.1 Учебная литература

Основная учебная литература

Башлы, П. Н. Информационная безопасность и защита информации : учебник / П. Н. Башлы, А.В. Бабаш, Е.К. Баранова. – Москва : РИОР, 2013. – 222 с. – ISBN 978-5-369-001178-2. – URL: http://znanium.com/bookread2.php?book=405000

Дополнительная учебная литература

Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2023. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511998.

Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2023. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511138.

Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2023. — 245 с. — (Высшее образование). — ISBN 978-5-9916-7090-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512423.

5.2 Материально-техническое и программное обеспечение дисциплины.

Учебные занятия по дисциплине проводятся в учебных аудиториях КГПИ ФГБОУ ВО «КемГУ»:

404 Учебная аудитория для проведения: - занятий лекционного типа; - групповых и индивидуальных консультаций; - текущего контроля и промежуточной аттестации. **Специализированная (учебная) мебель**: доска меловая, кафедра, столы, стулья. **Оборудование:** *переносное* - ноутбук, экран, проектор. **Используемое программное обеспечение:** MSWindows (MicrosoftImaginePremium 3 year по сублицензионному договору № 1212/КМР от 12.12.2018 г. до 12.12.2021 г.), LibreOffice (свободно распространяемое ПО), Яндекс.Браузер (отечественное свободно распространяемое ПО). **Интернет с обеспечением доступа в ЭИОС.**	Учебный корпус №4. 654079, Кемеровская область, г. Новокузнецк, пр-кт Металлургов, д. 19
502 Компьютерный класс. Учебная аудитория (мультимедийная) для проведения: - занятий лекционного типа; - занятий семинарского (практического) типа; - занятий лабораторного типа; - групповых и индивидуальных консультаций; - самостоятельной работы; - текущего контроля и промежуточной аттестации. **Специализированная (учебная) мебель**: доска меловая, столы компьютерные, стулья. **Оборудование для презентации учебного материала**: *стационарное* - компьютер, экран, проектор, наушники. **Лабораторное оборудование**: стационарное – компьютеры для обучающихся (16 шт.). **Используемое программное обеспечение**: MSWindows (MicrosoftImaginePremium 3 year по сублицензионному договору № 1212/КМР от 12.12.2018 г. до 12.12.2021 г.), LibreOffice (свободно распространяемое ПО), Firefox 14 (свободно распространяемое ПО), Яндекс.Браузер (отечественное свободно распространяемое ПО), MicrosoftVisualStudio (MicrosoftImaginePremium 3 year по сублицензионному договору № 1212/КМРот 12.12.2018 г. до 12.12.2021 г.), Среда статистических вычислений Rv.4.0.2 (свободно распространяемое ПО). **Интернет с обеспечением доступа в ЭИОС.**	Учебный корпус №4. 654079, Кемеровская область, г. Новокузнецк, пр-кт Металлургов, д. 19

5.3 Современные профессиональные базы данных и информационные справочные системы.

Перечень СПБД и ИСС по дисциплине

CITForum.ru - on-line библиотека свободно доступных материалов по информационным технологиям на русском языке - http://citforum.ru

Научная электронная библиотека eLIBRARY.RU – крупнейший российский информационный портал в области науки, технологии, медицины и образования, содержащий рефераты и полные тексты - www.elibrary.ru

База данных Science Direct (более 1500 журналов издательства Elsevier, среди них издания по математике и информатике), режим доступа :https://www.sciencedirect.com

6 Иные сведения и (или) материалы.

6.1.Примерные темы письменных учебных работ

6.1.1 Примерные задания для итогового теста

1. К техническим средствам добывания информации относятся средства

a) подслушивания, подглядывания, перехвата и физико-химического анализа;
b) подслушивания, наблюдения, перехвата и физико-химического анализа;
c) подслушивания, наблюдения, перехвата и компьютерные;
d) подслушивания, подглядывания, перехвата и программные.

2. Что относится к демаскирующим признакам?

a) признак расположения;
b) признак движения;
c) структурно-видовой признак;
d) признак заметности;
e) признак деятельности.

3. Физический, технический и программный уровни относятся к...

a) программному уровню;
b) программно-техническому уровню;
c) техническому уровню.

4. Конфиденциальность, целостность, доступность - это основные составляющие

a) информационной безопасности;
b) политики безопасности;
c) программы безопасности;
d) Доктрины информационной безопасности.

5. Тестирование на проникновение - это элемент

a) аудита информационной безопасности;
b) контроля информационной безопасности;
c) организации информационной безопасности.

6. Верно ли, что при оценке достоверности информации можно использовать такой критерий как "разборчивость речи"?

a) верно;

b) неверно.

6.1.2 Образец заданий для контрольной работы

Контрольная работа по разделу 2. Криптографические методы защиты информации

1. Зашифровать текст с помощью метода двойной перестановки.
2. Зашифровать текст с помощью магического квадрата.
3. Зашифровать текст с помощью шифра Цезаря.

Контрольная работа по разделу 3. Механизмы обеспечения информационной безопасности

1. Реализовать механизм электронной подписи документа.
2. Реализовать механизм аутентификации пользователя.
3. Реализовать схему подписи Шнорра.
4. Реализовать алгоритм RSA.
5. Реализовать алгоритм DES.

6.2. Примерные вопросы и задания / задачи для промежуточной аттестации

Семестр 5

Таблица 6 - Примерные теоретические вопросы и практические задания / задачи к зачету с оценкой

Разделы и темы	Примерные теоретические вопросы	Примерные практические задания / задачи
1. *Информационная безопасность*		
1.1 Составляющие информационной безопасности	1. Основные понятия информационной безопасности. 2. Проблема информационной безопасности общества. 3. Структура понятия «информационная безопасность». 4. Уровни формирования режима информационной безопасности.	1. Определить уровни режима информационной безопасности организации.
1.2 Угрозы информационной безопасности	1. Информационные угрозы, их виды и причины возникновения. 2. Классы несанкционированного доступа к информации. 3. Информационные угрозы для государства.	2. Определить угрозы информационной безопасности организации.
1.3 Безопасность персональных данных	1. Информационные угрозы для личности (физического лица). 2. Применение методов социальной инженерии для похищения персональных данных. 3. Вредоносные программы: понятие, классификация. 4. Защита от вредоносного ПО.	3. Составить концепцию фишингового письма для персонажа, пользуясь методами социальной инженерии.
1.4 Каналы утечки и искажения информации	5. Технические каналы утечки информации.	4. Составить алгоритм протоколирования всех нажатий клавиш и времени их нажатия в

		файл аудита клавиатуры.
1.5 Нормативно-правовые основы информационной безопасности	6. Государственное регулирование информационной безопасности. 7. Доктрина информационной безопасности РФ. 8. Стандарты информационной безопасности.	5. Сформулировать проблемы правового обеспечения создания и функционирования системы мониторинга угроз информационных атак на критически важные сегменты информационной инфраструктуры Российской Федерации
1.6 Информационная безопасность в компьютерных сетях	9. Классификация удаленных угроз. 10. Типовые удаленные атаки. 11. Защита информации в Интернете.	6. Составить модель типовой атаки «Троянский конь».
2. *Криптографические методы защиты информации*		
2.1 Основные понятия и история криптографии	12. Основные понятия криптографии. 13. Классическая задача криптографии. 14. Примеры применения криптографии.	7. Зашифровать текст шифром Цезаря.
2.2 Криптографические системы	15. Симметричные системы шифрования. 16. Блочные и поточные криптосистемы. 17. Асимметричные системы шифрования.	8. Составить алгоритм метода Эль-Гамаля. 9. Составить алгоритм Виженера.
2.3 Стеганография	18. История развития стеганографии. 19. Основные алгоритмы встраивания информации в изображение. 20. Основные алгоритмы встраивания информации в текст.	10. Составить алгоритм метода Куттера-Джордана-Боссена
2.4 Электронная цифровая подпись	21. Алгоритм электронной цифровой подписи. 22. Алгоритм проверки подлинности электронной цифровой подписи.	11. Составить алгоритм электронной цифровой подписи.
3. *Механизмы обеспечения информационной безопасности*		
3.1 Контроль целостности информации	23. Понятие «имитозащита». 24. Алгоритмы автоматического обнаружения ошибок при передаче данных.	12. Реализовать алгоритм контроля целостности с применением контрольных цифр.
3.2 Идентификация и аутентификация	25. Понятия *«идентификация» и «аутентификация».* 26. *Механизмы идентификации и аутентификации.* 27. *Биометрия.*	13. Составить алгоритм процедуры идентификации по схеме Шнорра. 14. Составить алгоритм процедуры аутентификации по схеме Шнорра.
3.3 Методы разграничения доступа	28. Разграничение доступа по уровням секретности. 29. Матрицы установления полномочий	15. Составить алгоритм метода разграничения доступа по спискам

Составитель (и): старший преподаватель кафедры МФММ Гаврилова Ю.С.

(*фамилия, инициалы и должность преподавателя (ей)*)