Подписано электронной подписью:
Вержицкий Данил Григорьевич
Должность: Директор КГПИ ФГБОУ ВО «КемГУ»
Дата и время: 2024-02-21 00:00:00
471086fad29a3b30e244c728abc3661ab35c9d5021b0dcf0e75e03a5b6fdf6436

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Кузбасский гуманитарно-педагогический институт
федерального государственного бюджетного образовательного учреждения
высшего образования
«Кемеровский государственный университет»

Факультет информатики, математики и экономики

УТВЕРЖДАЮ
Декан А.В. Фомина
10 февраля 2022 г.

Рабочая программа дисциплины

К.М.06.04 Математические методы и программное обеспечение защиты информации

Направление подготовки
01.03.02 Прикладная математика и информатика

Направленность (профиль) подготовки
ИНТЕЛЛЕКТУАЛЬНЫЙ АНАЛИЗ ДАННЫХ

Программа бакалавриата

Квалификация выпускника
бакалавр

Форма обучения
Очная

Год набора 2022

Новокузнецк 2022

Оглавление

1 Цель дисциплины. 3
1.1 Формируемые компетенции 3
1.2 Индикаторы достижения компетенций 3
1.3 Знания, умения, навыки (ЗУВ) по дисциплине 3
2 Объём и трудоёмкость дисциплины по видам учебных занятий. Формы промежуточной аттестации. 4
3. Учебно-тематический план и содержание дисциплины. 4
3.1 Учебно-тематический план 4
3.2. Содержание занятий по видам учебной работы 5
4 Порядок оценивания успеваемости и сформированности компетенций обучающегося в текущей и промежуточной аттестации. 7
5 Материально-техническое, программное и учебно-методическое обеспечение дисциплины. 8
5.1 Учебная литература 8
5.2 Материально-техническое и программное обеспечение дисциплины. 9
5.3 Современные профессиональные базы данных и информационные справочные системы. 9
6 Иные сведения и (или) материалы. 10
6.1.Примерные темы письменных учебных работ 10
6.2. Примерные вопросы и задания / задачи для промежуточной аттестации 11

1 Цель дисциплины.

В результате освоения данной дисциплины у обучающегося должны быть сформированы компетенции основной профессиональной образовательной программы бакалавриата (далее - ОПОП): ОПК-4.

Содержание компетенций как планируемых результатов обучения по дисциплине см. таблицы 1 и 2.

1.1 Формируемые компетенции

Таблица 1 - Формируемые дисциплиной компетенции

Наименование вида компетенции *(универсальная, общепрофессиональная, профессиональная)*	Наименование категории (группы) компетенций	Код и название компетенции
Общепрофессиональная	Информационно-коммуникационные технологии для профессиональной деятельности	ОПК-4 Способен решать задачи профессиональной деятельности с использованием существующих информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

1.2 Индикаторы достижения компетенций

Таблица 2 – Индикаторы достижения компетенций, формируемые дисциплиной

Код и название компетенции	Индикаторы достижения компетенции по ОПОП	Дисциплины и практики, формирующие компетенцию ОПОП
ОПК-4 Способен решать задачи профессиональной деятельности с использованием существующих информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК 4.1 Анализирует и описывает принципы работы и требования к современным информационным технологиям, информационным системам и системам искусственного интеллекта, используемым в профессиональной деятельности (по профилю программы) в условиях цифровой экономики в РФ. ОПК 4.2 Учитывает требования информационной безопасности при решении задач профессиональной деятельности. ОПК 4.3 Применяет информационно-коммуникационные технологии и информационные системы для решения задач профессиональной деятельности.	К.М.06.02 Языки и методы программирования К.М.06.03 Базы данных **К.М.06.04 Математические методы и программное обеспечение защиты информации** К.М.06.05 Программные средства визуализации данных К.М.06.06 Пакеты прикладных программ для 3D-моделирования К.М.06.07 Теория языков и трансляций К.М.06.08 Современные технологии программирования К.М.06.09 Программирование в системах реального времени К.М.09.01(У) Технологическая (проектно-технологическая) практика К.М.09.04(П) Технологическая (проектно-технологическая) практика К.М.09.05(Н) Научно-исследовательская работа

1.3 Знания, умения, навыки (ЗУВ) по дисциплине

Таблица 3 – Знания, умения, навыки, формируемые дисциплиной

Код и название компетенции	Индикаторы достижения компетенции, закрепленные за дисциплиной	Знания, умения, навыки (ЗУВ), формируемые дисциплиной
ОПК-4 Способен решать задачи профессиональной деятельности с использованием существующих информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК 4.2 Учитывает требования информационной безопасности при решении задач профессиональной деятельности. ОПК 4.3 Применяет информационно-коммуникационные технологии и информационные системы для решения задач профессиональной деятельности	**Знать:** – методы обеспечения информационной безопасности; – современные информационно-коммуникационные технологии. **Уметь**: – применять методы защиты информации при решении задач профессиональной деятельности. **Владеть**: – навыками обеспечения защиты информации в процессе решения задач профессиональной деятельности.

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

Таблица 4 – 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)	48
Аудиторная работа (всего):	48
в том числе:	
лекции	18
лабораторные работы	30
в интерактивной форме	
3 Самостоятельная работа обучающихся (всего)	60
4 Промежуточная аттестация обучающегося - экзамен (5 семестр)	36

3. Учебно-тематический план и содержание дисциплины.

3.1 Учебно-тематический план

Таблица 5 - 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.	практ.	лаб.		
Семестр 5							
	1. Информационная безопасность						Контрольная работа

№ 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.	практ.	лаб.		
1	1.1 Составляющие информационной безопасности	2	1			1	
2	1.2 Угрозы информационной безопасности	2	1			1	
3	1.3 Безопасность персональных данных	8			4	4	Защита отчета по ЛР №1,2
4	1.4 Каналы утечки и искажения информации	4			2	2	Защита отчета по ЛР №3
5	1.5 Нормативно-правовые основы информационной безопасности	4	2			2	
6	1.6 Информационная безопасность в компьютерных сетях	12	2		4	6	Защита отчета по ЛР №4,5
	2. Криптографические методы защиты информации						Контрольная работа
7	2.1 Основные понятия и история криптографии	12	2		4	6	Защита отчета по ЛР №6-7
8	2.2 Криптографические системы	20	4		4	12	Защита отчета по ЛР №8-10
9	2.3 Стеганография	16	2		4	10	Защита отчета по ЛР №11-13
10	2.4 Электронная цифровая подпись	8			4	4	Защита отчета по ЛР №14-15
	3. Механизмы обеспечения информационной безопасности						Контрольная работа
11	3.1 Контроль целостности информации	8	2		2	4	Защита отчета по ЛР №16
12	3.2 Идентификация и аутентификация	10	1		2	7	Защита отчета по ЛР №17-18
13	3.3 Методы разграничения доступа	2	1			1	
	Промежуточная аттестация	36					экзамен
	Всего:	**144**	**18**		**30**	**60**	**36**

3.2. Содержание занятий по видам учебной работы

Таблица 6 – Содержание дисциплины

№ п/п	Наименование раздела, темы дисциплины	Содержание занятия
	Семестр 5	
Содержание лекционного курса		
1	*Информационная безопасность*	
1.1	Составляющие информационной безопасности	*Понятие «информационная безопасность». Проблема информационной безопасности общества. Составляющие информационной безопасности: доступность, целостность, конфиденциальность. Уровни формирования режима информационной безопасности: законодательно-правовой, административный (организационный), программно-технический. Задачи информационной безопасности общества.*

№ п/п	Наименование раздела, темы дисциплины	Содержание занятия
1.2	Угрозы информационной безопасности	*Понятие «угроза информационной безопасности». Классы угроз информационной безопасности. Классы несанкционированного доступа к информации. Технические каналы утечки информации. Наиболее распространенные угрозы нарушения доступности, целостности и конфиденциальности информации. Понятие «вредоносное программное обеспечение», причины его появления. Классификация вредоносного программного обеспечения. История развития вредоносных программ. Антивирусное программное обеспечение: особенности работы, методы защиты, факторы, определяющие качество защиты.*
1.5	Нормативно-правовые основы информационной безопасности	*Правовые основы информационной безопасности общества. Нормативно-правовые основы информационной безопасности в РФ: Конституция РФ, Концепция национальной безопасности. Стандарты информационной безопасности.*
1.6	Информационная безопасность в компьютерных сетях	*Понятие «удаленная угроза». Цели сетевой безопасности. Методы и средства защиты в глобальных вычислительных сетях. Модель OSI: распределение функций безопасности по уровням. Классификация удаленных угроз. Типовые удаленные атаки.*
2	*Криптографические методы защиты информации*	
2.1	Основные понятия и история криптографии	*Основные понятия: криптография, криптоанализ, криптоаналитическая атака, компрометация криптосистемы, шифр, криптографическая система, криптографический протокол. Классическая задача криптографии.*
2.2	Криптографические системы	*Симметричные системы шифрования. Блочные криптосистемы: сети Фейстеля, блочный шифр DES, алгоритм шифрования IDEA, режим гаммирования, режим выработки имитовставки. Поточные криптосистемы: шифр гаммирования RC4.* *Асимметричные системы шифрования: схема асимметричного шифрования, алгоритм Диффи-Хеллмана, RSA, Эль-Гамаля.*
2.3	Стеганография	*История стеганографии. Методы встраивания информации в изображение, звук, текст.*
3	*Механизмы обеспечения информационной безопасности*	
3.1	Контроль целостности информации	*Понятие «имитозащита». Автоматическое обнаружение ошибок при передаче данных: самоконтролирующиеся коды. Коды с проверкой на четность, коды Хэмминга, циклические коды.*
3.2	Идентификация и аутентификация	*Понятия «идентификация» и «аутентификация». Механизмы идентификации и аутентификации. Биометрия.*
3.3	Методы разграничения доступа	*Методы разграничения доступа: по спискам, использование матрицы установления полномочий, разграничение доступа по уровням секретности и категориям, парольное разграничение доступа. Мандатное и дискретное управление доступом.*
Содержание лабораторных занятий		
1	*Информационная безопасность*	
1.3	Безопасность	Лабораторная работа №1. Защита персональных данных.

№ п/п	Наименование раздела, темы дисциплины	Содержание занятия
	персональных данных	Лабораторная работа №2. Техника фишинга.
1.4	Каналы утечки и искажения информации	Лабораторная работа №3. Аудит клавиатуры.
1.6	Информационная безопасность в компьютерных сетях	Лабораторная работа №4. Модель типовой атаки «Троянский конь». Лабораторная работа №5. Безопасность в компьютерных сетях.
2	*Криптографические методы защиты информации*	
2.1	Основные понятия и история криптографии	Лабораторная работа №6. Подстановочные перестановочные шифры. Лабораторная работа №7. Методы вскрытия шифров.
2.2	Криптографические системы	Лабораторная работа №8. Метод Эль Гамаля. Лабораторная работа №9. Криптосистема шифрования данных RSA. Лабораторная работа №10. Хеш-функция.
2.3	Стеганография	Лабораторная работа №11. Метод Куттера-Джордана-Боссена. Лабораторная работа №12. Метод Бенгама-Мемона-Эо-Юнга. Лабораторная работа №13. Методы извлечения встроенной информации.
2.4	Электронная цифровая подпись	Лабораторная работа №14. Создание цифровой подписи. Лабораторная работа №15. Проверка подлинности цифровой подписи.
3	*Механизмы обеспечения информационной безопасности*	
3.1	Контроль целостности информации	Лабораторная работа №16. Контроль целостности с применением битов четности.
3.2	Идентификация и аутентификация	Лабораторная работа №17. Процедуры идентификации/аутентификации на основе алгоритма RSA. Лабораторная работа №18. Процедуры идентификации/аутентификации по схеме Шнорра.
	Промежуточная аттестация - *экзамен*	

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 7.

Таблица 7 - 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 8)

Таблица 8 – 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

Голиков, А. М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А. М. Голиков. – Томск : ТУСУР, 2015. – 284 с. – URL: http://biblioclub.ru/index.php?page=book_view_red&book_id=480637

Сердюк, В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий : учебное пособие / В.А. Сердюк. – Москва : ИД Высшей школы экономики, 2011. – 574 с. – ISBN 978-5-7598-0698-1. – http://biblioclub.ru/index.php?page=book_view_red&book_id=440285

Спицын, В. Г. Информационная безопасность вычислительной техники : учебное пособие / В.Г. Спицын. – Томск : Эль Контент, 2011. – 148 с. – ISBN 978-5-4332-0020-3. – http://biblioclub.ru/index.php?page=book_view_red&book_id=208694

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

Информационная система «Единое окно доступа к информационным ресурсам» http://window.edu.ru/catalog/

Базы данных и аналитические публикации на портале «Университетская информационная система Россия», режим доступа: https://uisrussia.msu.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 9 - Примерные теоретические вопросы и практические задания / задачи к экзамену

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. Определить угрозы информационной безопасности организации.

	2. Классы несанкционированного доступа к информации. 3. Информационные угрозы для государства.	
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)*)