Подписано электронной подписью:
Вержицкий Данил Григорьевич
Должность: Директор КГПИ ФГБОУ ВО «КемГУ»
Дата и время: 2024-04-24 00:00:00
471086fad29a3b30e244c728abc3661ab35c9d50210dcf0e75e03a5b6fdf6436

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Кемеровский государственный университет»
Кузбасский гуманитарно-педагогический институт
федерального государственного бюджетного образовательного учреждения
высшего образования
«Кемеровский государственный университет»
Факультет информатики, математики и экономики

УТВЕРЖДАЮ
Декан
А. В. Фомина
8 февраля 2024 г.

Рабочая программа дисциплины

Б1.О.08 Математические методы и программное обеспечение защиты информации
Код, название дисциплины

Направление подготовки
02.03.03 Математическое обеспечение и администрирование информационных систем
Код, название направления

Направленность (профиль) подготовки
Программное и математическое обеспечение информационных технологий

Программа бакалавриата

Квалификация выпускника
бакалавр

Форма обучения
Очная

Год набора 2021

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.

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	Теоретические и практические основы профессиональной деятельности	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
Общепрофессиональная	Информационно-коммуникационные технологии для профессиональной деятельности	ОПК-3 Способен понимать и применять современные информационные технологии, в том числе отечественные, при создании программных продуктов и программных комплексов различного назначения

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-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	Б1.О.05 Дискретная математика Б1.О.08 Математические методы и программное обеспечение защиты информации Б1.О.11 Компьютерная графика Б1.О.14 Метрология и качество программного обеспечения Б1.О.19 Базы данных Б1.О.24 3D моделирование Б2.О.02(П) Технологическая (проектно-технологическая) практика Б3.01(Д) Подготовка к

Код и название компетенции	Индикаторы достижения компетенции по ОПОП	Дисциплины и практики, формирующие компетенцию ОПОП
		процедуре защиты и защита выпускной квалификационной работы
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 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	Б1.О.04 Информатика Б1.О.07 Языки и методы программирования Б1.О.08 Математические методы и программное обеспечение защиты информации Б1.О.10 Операционные системы Б1.О.16 Информационные системы и технологии Б1.О.19 Базы данных Б1.О.22 Программная инженерия Б1.О.23 Проектирование и разработка мобильных приложений Б2.О.01(У) Технологическая (проектно-технологическая) практика Б2.О.02(П) Технологическая (проектно-технологическая) практика Б3.01(Д) Подготовка к процедуре защиты и защита выпускной квалификационной работы

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-2 Способен применять современный математический аппарат,	2.2 Применяет методы проектирования,	**Знать:** - основные виды криптографических методов и алгоритмов, принципы их построения и

Код и название компетенции	Индикаторы достижения компетенции, закрепленные за дисциплиной	Знания, умения, навыки (ЗУВ), формируемые дисциплиной
связанный с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности	разработки, и реализации программных продуктов	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 3.5 Анализирует и описывает принципы работы и требования к современным ИТ, ИС, СИИ, используемых в профессиональной деятельности в условиях цифровой экономики	**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.

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	ОЗФО	ЗФО
1 Общая трудоемкость дисциплины	144		

2 Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	54		
Аудиторная работа (всего):			
в том числе:			
лекции	6		
практические занятия, семинары			
практикумы			
лабораторные работы	48		
в интерактивной форме			
в электронной форме			
Внеаудиторная работа (всего):			
в том числе, индивидуальная работа обучающихся с преподавателем			
подготовка курсовой работы /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)	90		
4 Промежуточная аттестация обучающегося	Зачет с оценкой – 7 семестр		

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				ЗФО			
			Аудиторн. занятия			СРС	Аудиторн. занятия		СРС	
			лекц.	практ.	лаб.		лекц	практ.		
Семестр 7										
	1. Информационная безопасность									Контрольная работа
1	1.1 Составляющие информационной безопасности	3	0,5			3				
2	1.2 Угрозы информационной безопасности	5	0,5			5				
3	1.3 Безопасность персональных данных	12			2	8				Защита отчета по ЛР №1,2
4	1.4 Каналы утечки и искажения информации	6			2	4				Защита отчета по ЛР №3
5	1.5 Нормативно-правовые основы информационной безопасности	6	1			6				
6	1.6 Информационная безопасность в	8	0,5		2	4				Защита отчета

№ недели п/п	Разделы и темы дисциплины по занятиям	Общая трудоёмкость *(всего час.)*	Трудоемкость занятий (час.)							Формы текущего контроля и промежуточной аттестации успеваемости
			ОФО				ЗФО			
			Аудиторн. занятия			СРС	Аудиторн. занятия		СРС	
			лекц.	практ.	лаб.		лекц	практ.		
	компьютерных сетях									по ЛР №4,5
	2. Криптографические методы защиты информации									Контрольная работа
7	2.1 Основные понятия и история криптографии	18	0,5		6	10				Защита отчета по ЛР №6-9
8	2.2 Криптографические системы	18	1		6	12				Защита отчета по ЛР №10-12
9	2.3 Стеганография	20	0,5		10	10				Защита отчета по ЛР №13-17
10	2.4 Электронная цифровая подпись	10			4	6				Защита отчета по ЛР №18-19
	3. Механизмы обеспечения информационной безопасности									Контрольная работа
11	3.1 Контроль целостности информации	20	0,5		10	9				Защита отчета по ЛР №20-24
12	3.2 Идентификация и аутентификация	15	0,5		6	9				Защита отчета по ЛР №25-27
13	3.3 Методы разграничения доступа	3	0,5			3				
	Промежуточная аттестация - *зачет с оценкой*									зачет с оценкой
ИТОГО по семестру 7		**144**	**6**		**48**	**90**				
	Всего:	**144**	**6**		**48**	**90**				

3.2. Содержание занятий по видам учебной работы

Таблица 6 – Содержание дисциплины

№ п/п	Наименование раздела, темы дисциплины	Содержание занятия
	Семестр 7	
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.*
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.*

№ п/п	Наименование раздела, темы дисциплины	Содержание занятия
		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 персональных данных	Лабораторная работа №1. Защита 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	Лабораторная работа №6. Подстановочные шифры.

№ п/п	Наименование раздела, темы дисциплины	Содержание занятия
	история криптографии	Лабораторная работа №7. Перестановочные шифры. Лабораторная работа №8. Методы вскрытия шифров. Лабораторная работа №9. Анализ стойкости шифров.
2.2	Криптографические системы	Лабораторная работа №10. Метод Эль Гамаля. Лабораторная работа №11. Криптосистема шифрования данных RSA. Лабораторная работа №12. Хеш-функция.
2.3	Стеганография	Лабораторная работа №13. Метод Куттера-Джордана-Боссена. Лабораторная работа №14. Метод Бенгама-Мемона-Эо-Юнга. Лабораторная работа №15. Метод изменения интервалов между предложениями. Лабораторная работа №16. Метод изменения количества пробелов в конце текстовых строк. Лабораторная работа №17. Методы извлечения встроенной информации.
2.4	Электронная цифровая подпись	Лабораторная работа №18. Создание цифровой подписи. Лабораторная работа №19. Проверка подлинности цифровой подписи.
3	*Механизмы обеспечения информационной безопасности*	
3.1	Контроль целостности информации	Лабораторная работа №20. Контроль целостности с применением битов четности. Лабораторная работа №21. Контроль целостности с применением контрольных цифр. Лабораторная работа №22. Контроль целостности с применением контрольных сумм. Лабораторная работа №23. Контроль целостности с применением кода коррекции ошибок. Лабораторная работа №24. Алгоритм DES-CBS.
3.2	Идентификация и аутентификация	Лабораторная работа №25. Процедуры идентификации/аутентификации на основе алгоритма RSA. Лабораторная работа №26. Процедуры идентификации/аутентификации по схеме Шнорра. Лабораторная работа №27. Процедуры идентификации/аутентификации по схеме Фейге-Фиата-Шамира.
	Промежуточная аттестация - *зачет с оценкой*	

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 - Шкала и показатели оценивания результатов учебной работы обучающихся по видам в балльно-рейтинговой системе (БРС) семестр 7

Учебная работа (виды)	Сумма баллов	Виды и результаты учебной работы	Оценка в аттестации (шкала и показатели оценивания)	Баллы
Текущая учебная	**80**	Посещение лекционных	**0,3 балла** - конспект 1 лекционного	5

работа в семестре (Посещение занятий по расписанию и выполнение заданий)		занятий (ведение конспекта) (18 лекций)	занятия	
		Лабораторные работы (отчет о выполнении лабораторной работы) (27 работ).	**0,5 балл** - выполнение работы на 51-65% **1 балл** – выполнение работы на 65,1-85% **1,5 балла** – выполнение работы на 85,1-100%	27 – 41
		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				51 - 80
Промежуточная аттестация (зачет с оценкой)	20	Тест.	**6 балла** (пороговое значение) **10 баллов** (максимальное значение)	6 - 10
		Решение задачи 1.	**2 балла** (пороговое значение) **5 баллов** (максимальное значение)	2 - 5
		Решение задачи 2.	**2 балла** (пороговое значение) **5 баллов** (максимальное значение)	2 - 5
Итого по промежуточной аттестации (зачету с оценкой)				10 – 20 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

1. 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 (дата обращения: 03.02.2023).

Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/530927 (дата обращения: 03.02.2023).

5.2 Материально-техническое и программное обеспечение

дисциплины.

Учебные занятия по дисциплине проводятся в учебных аудиториях КГПИ КемГУ:

615 Учебная аудитория (мультимедийная) для проведения: - занятий лекционного типа. **Специализированная (учебная) мебель:** доска меловая, кафедра, столы, стулья. **Оборудование для презентации учебного материала:** *стационарное* - компьютер, экран, проектор, акустическая система (колонки). **Используемое программное обеспечение:** Ubuntu Linux(свободно распространяемое ПО), LibreOffice (свободно распространяемое ПО), Яндекс.Браузер (отечественное свободно распространяемое ПО). **Интернет с обеспечением доступа в ЭИОС.**	654079, Кемеровская область, г. Новокузнецк, пр-кт Металлургов, д. 19
508 Компьютерный класс. Учебная аудитория (мультимедийная) для проведения: - занятий семинарского (практического) типа; - групповых и индивидуальных консультаций; - самостоятельной работы; - текущего контроля и промежуточной аттестации. **Специализированная (учебная) мебель:** доска меловая, кафедра, столы, стулья. **Оборудование для презентации учебного материала:** *стационарное* - компьютер преподавателя, проектор, экран. **Оборудование:** *стационарное* – компьютеры для обучающихся (18 шт.). **Используемое программное обеспечение:** MS Windows (Microsoft Imagine Premium 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), Opera 12 (свободно распространяемое ПО), Microsoft Visual Studio (Microsoft Imagine Premium 3 year по сублицензионному договору № 1212/КМР от 12.12.2018 г. до 12.12.2021 г.). **Интернет с обеспечением доступа в ЭИОС.**	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

Единое окно доступа к образовательным ресурсам - http://window.edu.ru/

6 Иные сведения и (или) материалы.

6.1.Примерные темы письменных учебных работ

Темы докладов (раздел 7. *Обеспечение информационной безопасности в ведущих зарубежных странах)*

1. Основные принципы обеспечения информационной безопасности в США.
2. Основные принципы обеспечения информационной безопасности в Великобритании.
3. Основные принципы обеспечения информационной безопасности в Швеции.
4. Основные принципы обеспечения информационной безопасности во Франции.
5. Основные принципы обеспечения информационной безопасности в Германии.
6. Основные принципы обеспечения информационной безопасности в Китае.
7. Основные принципы обеспечения информационной безопасности в Японии.
8. Основные принципы обеспечения информационной безопасности в Швейцарии.
9. Основные документы, регламентирующие обеспечение безопасности в США.
10. Основные документы, регламентирующие обеспечение безопасности в Великобритании.
11. Основные документы, регламентирующие обеспечение безопасности в Швеции.
12. Основные документы, регламентирующие обеспечение безопасности во Франции.
13. Основные документы, регламентирующие обеспечение безопасности в Германии.
14. Основные документы, регламентирующие обеспечение безопасности в Китае.
15. Основные документы, регламентирующие обеспечение безопасности в Японии.
16. Основные документы, регламентирующие обеспечение безопасности в Швейцарии.
17. Структура государственных органов обеспечения национальной информационной безопасности в США.
18. Структура государственных органов обеспечения национальной информационной безопасности в Великобритании.
19. Структура государственных органов обеспечения национальной информационной безопасности в Швеции.
20. Структура государственных органов обеспечения национальной информационной безопасности во Франции.
21. Структура государственных органов обеспечения национальной информационной безопасности в Германии.
22. Структура государственных органов обеспечения национальной информационной безопасности в Китае.
23. Структура государственных органов обеспечения национальной информационной безопасности в Японии.
24. Структура государственных органов обеспечения национальной информационной безопасности в Швейцарии.

6.2. Примерные вопросы и задания / задачи для промежуточной аттестации

Таблица 10 - Примерные теоретические вопросы и практические задания /

задачи к зачету с оценкой /экзамену

Семестр 7

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
Промежуточная аттестация – зачет с оценкой		

Составитель (и): Гаврилова Ю. С., старший преподаватель кафедры математики, физики и математического моделирования

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