МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ СИСТЕМ И БЕЗОПАСНОСТИ
Кафедра комплексной защиты информации

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Направление подготовки 10.03.01 Информационная безопасность
Направленность (профиль) Безопасность автоматизированных систем
(по отрасли или в сфере профессиональной деятельности)

Уровень высшего образования: бакалавриат
Форма обучения: очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2022

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ
Рабочая программа дисциплины

Составитель:
Кандидат технических наук, и.о. зав. кафедрой КЗИ Д.А. Митюшин

Ответственный редактор:
Кандидат технических наук, и.о. зав. кафедрой КЗИ Д.А. Митюшин

УТВЕРЖДЕНО
Протокол заседания кафедры
комплексной защиты информации
№ 8 от 31.03.2022

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины – обучение студентов основным принципам и подходам к использованию математического аппарата для криптографической и комплексной защиты информации.
Задачи дисциплины:

- научить определять и учитывать качественные и количественные особенности составляющих криптографической и комплексной защиты информации;
- сформировать у студентов представления о механизмах смены параметров криптографической защиты;
- научить решать основополагающие теоретико-практические задачи защиты информации с применением необходимого математического аппарата и сформировать математический подход к их решению;
- ознакомить студентов с математическими основами криптографических методов защиты компьютерной информации;
- ознакомить студентов с основными математическими принципами алгоритмов создания электронной цифровой подписи;
- ознакомить студентов с основными принципами построения систем комплексной защиты информации.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ПК-11 Способен проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	ПК-11.1 Знает методики проведения теоретических исследований уровней защищённости информационной безопасности объектов и систем	Знать: • основные понятия, методы, принципы, подходы, алгоритмы и приёмы криптографии и комплексной защиты информации;
	ПК-11.2 Умеет составлять и оформлять аналитический отчёт по проведённым испытаниям, делать выводы по оценке защищённости на основании аналитического отчёта	Уметь: • применять основные методы, принципы, подходы, алгоритмы и приёмы криптографии и комплексной защиты информации с необходимыми формулами для решения профессиональных математических задач
	ПК-11.3 Владеет навыками использования профиля защиты и задания по безопасности, формулирования выводов по оценке защищённости	Владеть: • основными подходами к постановке и решению задач, навыками математического описания профессиональных прикладных задач

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Математические основы защиты информации» относится к части, формируемой участниками образовательных отношений, блока дисциплин учебного плана.
Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: «Дискретная математика», «Матема-

тический анализ», «Теория вероятностей и математическая статистика», «Основы информационной безопасности».
В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: «Методы и средства защиты информации от утечки по техническим каналам», «Моделирование процессов и систем защиты информации», «Защита от несанкционированного доступа к информации в автоматизированных системах».

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет _3_ з.е., 108 академических часов.

Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
4	Лекции	**24**
4	Практические работы	**36**
	Всего:	**60**

Объем дисциплины в форме самостоятельной работы обучающихся составляет _48_ академических часа.

3. Содержание дисциплины

Раздел 1. Математический аппарат, используемый в криптографии

Тема 1. Основы одноключевых криптосистем

Основные понятия и определения криптографии. Обобщённая модель симметричной криптосистемы. Классификация угроз. Понятие о модели нарушителя. Принцип (правило) Кёркхоффа и его применение к одноключевым криптосистемам. Классификация методов шифрования информации. Криптозащита: при хранении информации, при передаче информации по каналу связи. Шифры простой замены; шифрующие таблицы Трисемуса. Шифры сложной замены; шифр Гронсфельда, система шифрования Вижинера, шифр “двойной квадрат” Уитстона. Шифрование перестановкой; использование маршрутов Гамильтона. Примеры. Различие между криптографией и стеганографией

Тема 2. Аналитический метод шифрования

Основные понятия аналитического (матричного) метода шифрования. Матричный (аналитический) метод шифрования-дешифрования. Примеры применения, особенности алгоритмической реализации метода. Понятия блочного и поточного шифрования и их основное отличие

Тема 3. Обратимость и теоретико-числовые основы криптографии

Обратимость как важное свойство, используемое в криптографии. Операция mod и её применение в задачах защиты информации. Алгоритм Евклида для отыскания наибольшего общего делителя. Вычисление обратных величин. Расширенный алгоритм Евклида и его применение. Конечные поля. Поле Галуа. Вычеты, кольца вычетов. Решение сравнений и систем сравнений. Функция Эйлера, теорема Эйлера. Понятие дискретного логарифма

Тема 4. Основы двухключевых криптосистем

Понятие о двухключевых асимметричных (несимметричных) криптосистемах. Обобщённая модель асимметричной криптосистемы в сравнении с симметричной криптосистемой. Алгоритм RSA и возможности его применения в двух режимах: шифрования (криптозащиты) и электронной цифровой подписи (ЭЦП)

Тема 5. Алгоритм RSA и его использование в режиме шифрования

Криптосистема RSA и её использование в режиме шифрования. Условно стойкие, вычислительно стойкие и безусловно стойкие шифры. Понятия односторонней (однонаправленной) функции и односторонней (однонаправленной) функции с потайным ходом (лазейкой). Задача факторизации и криптосистема (алгоритм) RSA

Тема 6. Использование известных двухключевых асимметричных криптосистем в режиме электронной цифровой подписи

Понятия односторонней (однонаправленной) хеш-функции и электронной цифровой подписи и основные требования к ним. Некоторые вопросы аутентификации. Использование криптосистемы RSA в режиме электронной цифровой подписи

Тема 7. Понятие о схемах разделения секрета и (древне)китайская теорема об остатках

(Древне)китайская теорема об остатках и возможности её использования в целях защиты информации. Задача о безопасном сохранении числового ключа между двумя компаньонами. Понятие совершенной схемы разделения секрета (совершенной СРС). Представление о пороговых схемах разделения секрета

Раздел 2. Математический аппарат для задач комплексной защиты информации

Тема 8. Элементы теории конечных автоматов и понятие об автоматной модели системы защиты GM

Распознавание множеств автоматами. Представление событий в автоматах. Основные проблемы абстрактной теории автоматов. Понятие об автоматной модели системы защиты GM и возможные направления её модернизации

Тема 8.2. Оптимизационная задача о назначениях и разбиение на классы для объектов доступа и субъектов доступа

Оптимизационная задача о назначениях. Венгерский метод решения задачи о назначениях. Оптимизация наборов прав пользователей при матричном принципе управления доступом и комплексной защите информации. Возможности разбиения на классы для объектов и субъектов доступа

Тема 9. Представления о расширенной модели безопасности Take-Grant

Отличительные особенности матричного и мандатного принципов управления доступом в компьютерных системах. Представления о расширенной модели безопасности Take-Grant и возможные направления её дальнейшей модернизации

Тема 10. Модель безопасности информационных потоков и другие модели безопасности

Модель безопасности информационных потоков при использовании мандатного принципа управления доступом. Другие модели безопасности: модель Low-Water-Mark, модель “Китайской стены” (Брюэра и Нэша) и возможные направления модернизации моделей

Тема 11. Модели контроля целостности информации и контроль доступа, базирующийся на ролях

Модели контроля целостности: модель Биба в сопоставлении с моделью Кларка-Вилсона и возможные направления их модернизации. Контроль доступа, базирующийся на ролях и его актуальность для вычислительной системы организации, пример для медицинского учреждения

Тема 12. Расчётные соотношения для контролируемой и неконтролируемой преград комплексной защиты информации

Расчётные соотношения для контролируемой и неконтролируемой преград комплексной защиты информации в случаях однозвенной (элементарной) и многозвенной защиты. Защита штатного входа в систему и прочность защитной преграды, основные расчётные соотношения и их использование. Случай многоуровневой защиты

Тема 13. Понятие о сложностных классах задач в ракурсе защиты компьютерной информации

Возможности приближенной оценки сложности алгоритмов защиты информации на основе сравнения порядка функций, принятого в математическом анализе. Классы P и NP; полиномиальный и недетерминировано-полиномиальный классы задач. Понятие оценки вычислительной сложности “в лучшем”, “в худшем” и “в среднем”

4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	2	3	4
1.	Основы одноключевых криптосистем.	Лекция 1. Практическое занятие 1. Самостоятельная работа.	Вводная лекция – теоретическая справка с кратким изложением основных понятий. Вводное занятие – теоретическая справка с кратким изложением основных понятий и решением задач. Дискуссия.
2	Аналитический метод шифрования.	Лекция 2. Практическое занятие 2. Самостоятельная работа.	Лекция с разбором конкретных ситуаций. Решение задач у доски с обсуждением. Консультирование.
3	Обратимость и теоретико-числовые основы криптографии.	Лекция 3. Практическое занятие 3. Самостоятельная работа.	Лекция с разбором конкретных ситуаций. Теоретическая справка с кратким изложением основных понятий и решением задач. Консультирование.
4	Основы двухключевых криптосистем	Лекция 4. Практическое занятие 4. Самостоятельная работа.	Лекция с разбором конкретных ситуаций. Практическое занятие с использованием частично-поисковых методов обучения. Дискуссия.
5	Алгоритм RSA и его ис-	Лекция 5.	Лекция с использованием ча-

	пользование в режиме шифрования.	Практическое занятие 5 Самостоятельная работа	стично-поисковых методов обучения. Самостоятельное моделирование задач с последующим их обсуждением и оптимизацией.
6	Использование известных двухключевых асимметричных криптосистем в режиме электронной цифровой подписи	Лекция 6. Практическое занятие 6. Самостоятельная работа.	Лекция с разбором конкретных ситуаций. Практическое занятие с использованием частично-поисковых методов обучения. Консультирование.
7	Понятие о схемах разделения секрета и (древне)китайская теорема об остатках.	Лекция 7. Практическое занятие 7. Самостоятельная работа.	Доклады с презентациями. Теоретическая справка с кратким изложением основных понятий. Решение задач у доски с обсуждением. Дискуссия. Консультирование.
8	Элементы теории конечных автоматов и понятие об автоматной модели системы защиты GM	Лекция 8.1. Практическое занятие 8.1 Самостоятельная работа.	Лекция с использованием частично-поисковых методов обучения. Семинар с использованием частично-поисковых методов обучения. Дискуссия.
9	Оптимизационная задача о назначениях и разбиение на классы для объектов доступа и субъектов доступа.	Лекция 8.2. Практическое занятие 8.2. Самостоятельная работа.	Лекция с разбором конкретных ситуаций. Решение задач у доски с обсуждением. Консультирование.
10	Представления о расширенной модели безопасности Take-Grant.	Лекция 9. Практическое занятие 9.	Лекция с разбором конкретных ситуаций. Дискуссия. Теоретическая справка с кратким изложением основных понятий. Решение задач у доски с обсуждением.

		Самостоятельная работа.	Дискуссия.
11	Модель безопасности информационных потоков и другие модели безопасности.	Лекция 10. Практическое занятие 10. Самостоятельная работа.	Лекция с разбором конкретных ситуаций. Теоретическая справка с кратким изложением основных понятий. Дискуссия. Решение задач у доски с обсуждением. Консультирование посредством электронной почты.
12	Модели контроля целостности информации и контроль доступа, базирующийся на ролях.	Лекция 11. Практическое занятие 11. Самостоятельная работа.	Теоретическая справка с кратким изложением основных понятий. Дискуссия. Консультирование посредством электронной почты.
13	Расчётные соотношения для контролируемой и неконтролируемой преград комплексной защиты информации.	Лекция 12. Практическое занятие 12. Самостоятельная работа.	Лекция с разбором конкретных ситуаций. Теоретическая справка с кратким изложением основных понятий и решением задач. Дискуссия.
14	Понятие о сложностных классах задач в ракурсе защиты компьютерной информации.	Лекция 13. Практическое занятие 13. Самостоятельная работа.	Теоретическая справка с кратким изложением основных понятий Теоретическая справка с кратким изложением основных понятий и решением задач. Консультирование.

В период временного приостановления посещения обучающимися помещений и территории РГГУ для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

– видео-лекции**;**

– онлайн-лекции в режиме реального времени;

– электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;

– системы для электронного тестирования;

– консультации с использованием телекоммуникационных средств.

5. Оценка планируемых результатов обучения

5.1 Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль:		
- аудиторный письменный тест	15 баллов	30 баллов
- аудиторная практическая работа (домашняя либо аудиторная)	20 баллов	20 баллов
- посещаемость теоретических и практических занятий	10 баллов	10 баллов
Промежуточная аттестация – зачет (зачет по билетам)		40 баллов
Итого за семестр		100 баллов

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2 Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A,B	зачтено	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	зачтено	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
67-50/ D,E	зачтено	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3 Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Промежуточная аттестация (примерные вопросы к зачёту) – проверка сформированности компетенций – ПК-11)

№	Вопрос	Реализуемая компетенция
1.	Понятие ключа шифрования, принцип (правило) Кёркхоффа и его применение к одноключевым криптосистемам.	ПК-11
2.	Алгоритм Евклида и его применение.	ПК-11
3.	Обратимость как важное свойство, используемое в криптографии. Вычисление обратных величин. Расширенный алгоритм Евклида и его применение.	ПК-11
4.	Основы одноключевых криптосистем.	ПК-11
5.	Шифр Трисемуса и шифр Гронсфельда, примеры.	ПК-11
6.	Шифр Гронсфельда и алгоритм RSA.	ПК-11
7.	Шифр "двойной квадрат" Уитстона и шифр Гронсфельда, примеры.	ПК-11
8.	Шифр Вижинера и шифр Гронсфельда.	ПК-11
9.	Матричный (аналитический) метод шифрования-дешифрования.	ПК-11
10.	Асимметричные криптосистемы.	ПК-11
11.	Криптосистема (алгоритм) RSA.	ПК-11
12.	Функция Эйлера и её применение в криптосистеме (алгоритме) RSA.	ПК-11
13.	Задача факторизации и криптосистема (алгоритм) RSA.	ПК-11
14.	(Древне)китайская теорема об остатках и возможности её использования в целях защиты информации.	ПК-11
15.	Операция mod и её использование в криптографии.	ПК-11

16.	Вычисление обратных величин.	ПК-11
17.	Отличие между криптосистемой и схемой разделения секрета, примеры.	ПК-11
18.	Односторонняя функция, заложенная в основу криптосистемы RSA.	ПК-11
19.	Схема разделения секрета на основе (древне)китайской теоремы об остатках.	ПК-11
20.	Возможности представления компьютерных программ графами: области отладки программы и их сравнительная характеристика.	ПК-11
21.	Понятия кольца, вычета, поля Галуа.	ПК-11
22.	Модель безопасности Белла-Лападула и возможные направления её совершенствования.	ПК-11
23.	Модель “Китайской стены” (Брюэра и Нэша).	ПК-11
24.	Шифрование маршрутами Гамильтона.	ПК-11
25.	Решение сравнений.	ПК-11
26.	Решение систем сравнений.	ПК-11
27.	Прочность защитной преграды. Основные расчётные соотношения для однозвенной защиты (при атаках одним злоумышленником и организованной группой злоумышленников). Понятие о многоуровневой защите и понятие многозвенной защиты.	ПК-11

Тест№0 1 (проверка сформированности компетенций – ПК-11)
Вариант 0

1. Равнозначными (синонимами) являются следующие понятия:
A) симметричное шифрование и шифрование с открытым ключом;
B) несимметричное шифрование и асимметричное шифрование;
C) двухключевое шифрование с открытым ключом и асимметричное шифрование;
D) несимметричное шифрование и шифрование с секретным ключом.
2. В общем случае криптоалгоритм RSA:
A) работает быстрее одноключевых криптоалгоритмов;
B) работает медленнее одноключевых криптоалгоритмов;
C) работает с той же скоростью, что и одноключевые криптоалгоритмы;
D) ничего из перечисленного.
3. Существуют ли понятие пороговых схем разделения секрета:
A) да;
B) нет;
C) постановка вопроса некорректна;
D) требуется дополнительное исследование.
4. Бывают шифры:
A) простой замены;
B) сложной замены;
C) перестановки;
D) основанные на трудности решения задачи факторизации.
5. Метод шифрования маршрутами Гамильтона:
A) характеризуется тем, что в нём длина каждого блока обязательно равна 4;
B) характеризуется тем, что в нём длина каждого блока обязательно равна 3;
C) характеризуется тем, что в нём используется таблица;
D) характеризуется тем, что в нём в любом случае бессмысленно использовать неорграф-таблицу, а применяются только орграфы.
6. Понятие матрицы-ключа:
A) не существует;
B) существует;

C) существует и её размерность всегда 3x3 или 2x2;
D) существует и обычно она квадратная.
7. Шифрование с помощью таблицы Трисемуса является:
A) монограммным; B) биграммным; C) зависит только от размеров таблицы;
D) ничего из перечисленного.
8. В аналитическом (матричном) методе шифрования:
A) один ключ; B) несколько ключей, каждый из которых – элемент матрицы-ключа;
C) нет ни одного ключа;
D) два ключа.
9. В системе шифрования Вижинера длина ключа:
A) не может превышать 4;
B) всегда равна 4;
C) может превышать 4;
D) всегда нулевая.
10. В шифре “двойной квадрат” Уитстона обе таблицы:
A) могут быть только прямоугольными;
B) могут быть только квадратными;
C) могут иметь различающееся между 1-й и 2-й таблицами количество строк;
D) ничего из перечисленного.

Тест№2 (проверка сформированности компетенций – ПК-11)

Вариант 0

1. В классическом варианте задачи о назначениях матрица стоимостей C:
A) имеет размерность 3x3; B) квадратная; C) имеет размерность 2x2; D) отсутствует.
2. К задачам целочисленного программирования имеют отношение:
A) задача об оптимальном распределении заданий по трём компьютерам, работающим в сети;
B) задача о матричном принципе оптимального управления доступом в ОС WindowsXP;
C) директивные сроки выполнения работ либо оказания услуг;
D) ничего из перечисленного.
3. Существует ли понятие “тени” защищаемого схемой разделения секрета ключа:
A) да;
B) нет;
C) постановка вопроса некорректна;
D) существует синоним это понятия?
4. Возможны схемы разделения секрета:
A) основанные только на древнекитайской теореме об остатках, ибо другие так и не созданы;
B) основанные на любых теоремах;
C) геометрической природы;
D) с количеством участников как менее 10, так и более 10.
5. Всегда ли в схемах разделения секрета у каждого из участников одинаковые доли секрета:
A) да;
B) нет;
C) зависит только от значения числового ключа;
D) постановка вопроса некорректна?
6. В используемых в основанной на древнекитайской теореме об остатках схеме разделения секрета выражениях $(N_1 \cdot M_1)(\mathrm{mod}\, m_1) \equiv 1$ и $(N_2 \cdot M_2)(\mathrm{mod}\, m_2) \equiv 1$ числа N_1 и N_2:
A) могут совпасть;
B) не могут и не должны совпадать;
C) обычно никак не используются;
D) всегда одинаковы.
7. Классом вычетов по модулю m для данного модуля:
A) являются все целые числа, сравнимые по modm;

B) являются не все целые числа, сравнимые по modm;
C) является лишь меньшая часть целых чисел, сравнимых по modm
D) ничего из перечисленного.
8. Допустимо ли для краткости, когда вместо указания всего класса вычетов приводится только один его представитель:
A) да;
B) нет;
C) требуется дополнительное исследование;
D) постановка вопроса некорректна?
9. Если модуль является составным числом, то верно ли, что для каждого вычета имеется к нему обратный:
A) да; B) нет;
C) требуется дополнительное исследование;
D) постановка вопроса некорректна?
10. Допустимо ли меньшее (по абсолютному значению) число делить на большее (целочисленно с остатком):
A) да; B) нет;
C) требуется дополнительное исследование; D) тавтология?

Примерный вариант контрольной (самостоятельной аудиторной) работы (проверка сформированности компетенций – ПК-11)

Вариант 0

1. Используя схему разделения секрета, основанную на (древне)китайской теореме об остатках, защитить общий для двух компаньонов ключ *K*. (При отыскании *N* из выражений вида $(N \cdot M)(\mathrm{mod}\, m) = 1$ следует применить любые два из трёх изученных способов – поочерёдная проверка значений, вычисление на основе функции Эйлера при использовании алгоритма быстрого возведения в степень, расширенный алгоритм Евклида).

Вариант	1	2	3	4
Ключ *K*	9	13	14	15

2. Применяя расширенный алгоритм Евклида, найти обратный элемент a^{-1} по модулю *m* (при условии его существования) и проверить, что найденные числа *u, v* удовлетворяют равенству $au + mv = 1$.

Вариант	1	2	3	4
a	9	31	10	35
m	11	73	11	82

3. Зашифровать и расшифровать сообщение методом матричной алгебры (аналитическим методом шифрования), если заданы сообщения

Вариант	1	2	3	4
Сообщение	СЕКРЕТ	КНИЖКА	ПОДЪЁМ	ЛЖИВЫЙ

и матрица-ключ (для любого из вариантов) $A = \begin{pmatrix} 6 & 9 & 1 \\ 3 & 9 & 7 \\ 5 & 7 & 9 \end{pmatrix}$.

Билет для зачёта N^{0}0 (проверка сформированности компетенций – ПК-11)

1. Схема разделения секрета является совершенной, если:
A) произвольное множество участников полностью раскрывает секрет;
B) произвольное множество участников в результате своих действий по раскрытию секрета не получает о нём никакой дополнительной информации;
C) произвольное множество участников либо полностью раскрывает секрет, либо в результате не получает о нём никакой дополнительной информации;
D) ничего из перечисленного. (до 4 баллов)
2. В пороговых схемах разделения секрета:
A) обязательно все участники должны объединить свои усилия для совместного получения доступа к объекту защиты;
B) обязательно большинство участников должны объединить свои усилия для совместного получения доступа к объекту защиты;
C) обязательно меньшинство участников должны объединить свои усилия для совместного получения доступа к объекту защиты;
D) ничего из перечисленного. (до 4 баллов)
3. Древнекитайскую теорему об остатках:
A) нельзя использовать в схеме разделения секрета, если количество участников более 2-х;
B) можно использовать в схеме разделения секрета, если количество участников более 2-х;
C) можно использовать исключительно для разделения секрета;
D) ничего из перечисленного. (до 4 баллов)
4. Центр распределения ключей:
A) всегда нежелательно использовать при разделении секрета;
B) никогда не используют при разделении секрета;
C) используют исключительно тогда, когда разделение секрета происходит на основе древнекитайской теоремы об остатках;
D) ничего из перечисленного. (до 4 баллов)

5. Функция Эйлера и её применение в криптосистеме (алгоритме) RSA. (до 5 баллов)

6. Модель Кларка-Вилсона. (до 5 баллов)

7. Используя схему разделения секрета, основанную на (древне)китайской теореме об остатках, защитить общий для двух компаньонов ключ *K=24*. (При отыскании*N* из выражений вида $(N \cdot M) \pmod m = 1$ рекомендуется применить любые два из трёх изученных способов – поочерёдная проверка значений, вычисление на основе функции Эйлера при использовании алгоритма быстрого возведения в степень, расширенный алгоритм Евклида). (до 7 баллов)

8. Применяя расширенный алгоритм Евклида, найти обратный элемент a^{-1} по модулю *m=19* для *a=181* (при условии его существования) и проверить, что найденные числа *u, v* удовлетворяют равенству $au + mv = 1$. (до 7 баллов)

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Список источников и литературы

Литература

Основная

1. Введение в криптографию. Курс лекций / В.А. Романьков. – 2-еизд., испр. и доп. – М. : ФОРУМ : ИНФРА-М, 2018. – 240 с. – (Высшее образование:Бакалавриат). – Режим доступа: http://znanium.com/catalog/product/924700.

2. Кнауб, Л.В. Теоретико-численные методы в криптографии [Электронный ресурс]: Учеб.пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. – Красноярск : Сибирский федеральный университет, 2011. – 160 с. – ISBN 978-5-7638-2113-7. – Режим доступа: http://znanium.com/catalog/product/441493.

3. Алексеев, А.П. Курсовое проектирование для криптографов: учебное пособие / А.П. Алексеев. – М.: СОЛОН-Пр., 2018. – 100 с. - (Библиотека студента). – ISBN 978-5-91359-314-6. - Режим доступа: http://znanium.com/catalog/product/1015063.

4. Проектирование информационных систем [Электронный ресурс] : учебное пособие для бакалавриата по направлению подготовки 230700 - Прикладная информатика по профилям: Прикладная информатика в информационной сфере ; Прикладная информатика в экономике / Минобрнауки России, Федер. агентство по образованию, Гос. образоват. учреждение высш. проф. образования "Рос.гос. гуманитарный ун-т" (РГГУ), Ин-т информ. наук и технологий безопасности, Фак. информатики, Каф. информ. технологий ; [авт.: В. А. Лекае]. – Электрон.дан. - М. : РГГУ, 2013. - 360 с. - Режим доступа : http://elib.lib.rsuh.ru/elib/000008060. - ISBN 978-5-7281-1517-5. -С. 89-123.

5. Усенко О.А. Приложения теории информации и криптографии в радиотехнических системах: учебное пособие. – Ростов-на-Дону; Таганрог: Изд-во Южного федерального университета, 2017. - ISBN 978-5-9275-2569-0. - Режим доступа: http://znanium.com/catalog/product/1021618 .

Дополнительная

1. Гришина Н. В. Информационная безопасность предприятия: Учебное пособие. - Москва : Издательство "ФОРУМ" : ООО "Научно-издательский центр ИНФРА-М", 2017. - 239 с. - ISBN 978-5-00091-007-8. - Режим доступа: http://znanium.com/go.php?id=612572. – С. 28-197.

2. Информационная безопасность и защита информации: учеб.пособие / Баранова Е.К., Бабаш А.В. — 3-е изд., перераб. и доп. — М. : РИОР : ИНФРА-М, 2017. – 322 с. – (Высшее образование). – ww.dx.doi.org/10.12737/11380. - Режим доступа: http://znanium.com/catalog/product/763644.

3. Ищейнов В. Я. Основные положения информационной безопасности : Учебное пособие. - Москва : Издательство "ФОРУМ" : ООО "Научно-издательский центр ИНФРА-М", 2018. - 208 с. - ISBN 9785000914892. - Режим доступа: http://znanium.com/go.php?id=927190. – С. 57-89.

4. Шептунов М.В. Дискретная математика для бакалавриата. Учебное пособие для ВУЗов. – М.: Горячая линия – Телеком, 2017. (Гриф ФИРО).

6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Журнал “Прикладная дискретная математика”: http://journals.tsu.ru/pdm/&journal_page=archive;
2. Журнал “Математические вопросы криптографии”: http://www.mathnet.ru/php/archive.phtml?jrnid=mvk&wshow=contents&option_lang=rus .

Национальная электронная библиотека (НЭБ) www.rusneb.ru
ELibrary.ru Научная электронная библиотека www.elibrary.ru
Электронная библиотека Grebennikon.ru www.grebennikon.ru
Cambridge University Press
ProQuest Dissertation & Theses Global
SAGE Journals
Taylor and Francis
JSTOR

6.3 Профессиональные базы данных и информационно-справочные системы

Доступ к профессиональным базам данных: https://liber.rsuh.ru/ru/bases

Информационные справочные системы:
1. Консультант Плюс
2. Гарант

7. Материально-техническое обеспечение дисциплины

Для обеспечения дисциплины используется материально-техническая база образовательного учреждения: учебные аудитории, оснащённые доской, компьютером или ноутбуком, проектором (стационарным или переносным) для демонстрации учебных материалов.

Состав программного обеспечения:
1. Windows
2. Microsoft Office
3. Kaspersky Endpoint Security

Желательно использование проектора произвольного типа с операционной системой Windows на ПК и установленной на нём программой PowerPoint любых версий для (отдельных) презентаций во время лекций.

Для проведения занятий лекционного типа предлагаются тематические иллюстрации в формате презентаций PowerPoint.

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением или могут быть заменены устным ответом; обеспечивается индивидуальное равномерное освещение не менее 300 люкс; для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; письменные задания оформляются увеличенным шрифтом; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.
- для глухих и слабослышащих: лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования; письменные задания выполняются на компьютере в письменной форме; экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.
- для лиц с нарушениями опорно-двигательного аппарата: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с

учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих: в печатной форме увеличенным шрифтом, в форме электронного документа, в форме аудиофайла.
- для глухих и слабослышащих: в печатной форме, в форме электронного документа.
- для обучающихся с нарушениями опорно-двигательного аппарата: в печатной форме, в форме электронного документа, в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих: устройством для сканирования и чтения с камерой SARA CE; дисплеем Брайля PAC Mate 20; принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих: автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих; акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата: передвижными, регулируемыми эргономическими партами СИ-1; компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1 Планы практических занятий

Цель практических занятий – предоставление возможностей для углубленного изучения теории, овладения практическими навыками и выработки самостоятельного творческого мышления у студентов.

Задачи практических занятий:

отражение в учебном процессе современных достижений науки;

углубление теоретической и практической подготовки студентов;

- приближение учебного процесса к реальным условиям работы того или иного специалиста;
- формирование умения применять полученные знания на практике, осуществлять вычисления и расчёты;
- развитие инициативы и самостоятельности студентов;
- формирование навыков публичного выступления, способности представлять результаты проведённого исследования, умения вести дискуссию;
- контроль за освоением учебной дисциплины.

Функции практических занятий:

учебно-познавательная - закрепление, расширение, углубление знаний, полученных на лекциях и в ходе самостоятельных занятий;

обучающая - школа публичного выступления, развитие навыков отбора и обобщения информации;

стимулирующая - определённый стимул к дальнейшей пробе своих творческих сил и подготовке к более активной работе;

воспитательная - формирование мировоззрении и убеждений, воспитание самостоятельности, научного поиска, состязательности, смелости;

контролирующая - в проверке уровня знаний и качества самостоятельной работы студента.

Обучение студентов на практических занятиях направлено на:

- обобщение, систематизацию, углубление, закрепление полученных теоретических знаний по дисциплине;
- формирование умений (аналитических, проектировочных, конструктивных и др.) применять полученные знания на практике;
- реализацию единства интеллектуальной, практической деятельности;
- формирование практических умений выполнять определенные действия, операции, необходимые в последующей профессиональной деятельности;
- выработку при решении поставленных задач таких профессионально значимых факторов, как самостоятельность, ответственность, точность.

Тема 1 (3 ч.). Основы одноключевых криптосистем (проверка сформированности компетенций – ПК-11)

Задания:

1. Выяснить ключевые особенности, подходы, приёмы, алгоритмы, методы, модели, критерии и показатели для решения задач дисциплины, оформив в виде таблиц для каждого случая.

2. Научиться оценивать границы применимости основных подходов, приёмов, алгоритмов, методов, моделей, критериев и показателей для решения задач дисциплины – её разделов “Математический аппарат, используемый в криптографии” и “Математический аппарат для задач комплексной защиты информации”.

Тема 2 (3 ч.). Аналитический метод шифрования (проверка сформированности компетенций – ПК-11)

Задания:

1. Выяснить ключевые особенности метода для решения задач по теме занятия, оформив в виде таблиц для каждого случая.

2. Оценить границы применимости метода для решения задач по теме занятия.

3. Обсудить и проанализировать основные подходы к решению задач по теме занятия.

4. Попрактиковаться в грамотной постановке задач, учитывающих особенности комплексной защиты объектов информатизации, соотносящихся с изучаемой дисциплиной, с учётом основных требований выпускающей кафедры “Комплексная защита информации” (например,задействуядвукратноешифрование на основе изученного метода).

Тема 3 (4 ч.). Обратимость и теоретико-числовые основы криптографии (проверка сформированности компетенций –ПК-11)

Задания:

1. Выяснить ключевые особенности, подходы, приёмы, алгоритмы, методы, модели, критерии и показатели для решения задач по теме занятия, оформив в виде таблиц для каждого случая.

2. Оценить границы применимости основных подходов, приёмов, алгоритмов, методов, моделей, критериев и показателей для решения задач по теме занятия.

3. Обсудить и проанализировать основные подходы к решению задач по теме занятия.

4. Попрактиковаться в грамотной постановке задач, учитывающих особенности комплексной защиты объектов информатизации, соотносящихся с изучаемой дисциплиной, с учётом основных требований выпускающей кафедры “Комплексная защита информации”.

Тема 4 (2 ч.). Основы двухключевых криптосистем (проверка сформированности компетенций – ОПК-3, ПК-11)

Задания:

1. Выяснить ключевые особенности, подходы, приёмы, алгоритмы, методы, модели, критерии и показатели для решения задач по теме занятия, оформив в виде таблиц для каждого случая.

2. Оценить границы применимости основных подходов, приёмов, алгоритмов, методов, моделей, критериев и показателей для решения задач по теме занятия.

3. Обсудить и проанализировать основные подходы к решению задач по теме занятия.

4. Попрактиковаться в грамотной постановке задач, учитывающих особенности комплексной защиты объектов информатизации, соотносящихся с изучаемой дисциплиной, с учётом основных требований выпускающей кафедры “Комплексная защита информации”.

Тема 5 (2 ч.). Алгоритм RSAи его использование в режиме шифрования (проверка сформированности компетенций – ПК-11)

Задания:

1. Выяснить ключевые особенности, подходы, приёмы, алгоритмы, методы, модели, критерии и показатели для решения задач по теме занятия, оформив в виде таблиц для каждого случая.

2. Оценить границы применимости основных подходов, приёмов, алгоритмов, методов, моделей, критериев и показателей для решения задач по теме занятия.

3. Обсудить и проанализировать основные подходы к решению задач по теме занятия.

4. Попрактиковаться в грамотной постановке задач, учитывающих особенности комплексной защиты объектов информатизации, соотносящихся с изучаемой дисциплиной, с учётом основных требований выпускающей кафедры “Комплексная защита информации”.

Тема 6 (2 ч.). Использование известных двухключевых асимметричных криптосистем в режиме электронной цифровой подписи (проверка сформированности компетенций –ПК-11)

Задания:

1. Выяснить ключевые особенности, подходы, приёмы, алгоритмы, методы, модели, критерии и показатели для решения задач по теме занятия, оформив в виде таблиц для каждого случая.

2. Сделать доклад(ы) по теме занятия.

3. Членам группы научиться грамотно задавать вопросы докладчикам по теме выступления.

4. Выявить в ходе обсуждения основные достоинства и недостатки изложенного докладчиками материала.

5. Предложить свои рекомендации по устранению недостатков изложенного с позиций комплексной защиты объектов информатизации.

Тема 7 (2 ч.). Понятие о схемах разделения секрета и (древне)китайская теорема об остатках (проверка сформированности компетенций – ПК-11)

Задания:

1. Выяснить ключевые особенности, подходы, приёмы, алгоритмы, способы, критерии и показатели для решения задач по теме занятия, оформив в виде таблиц для каждого случая.

2. Оценить границы применимости основных подходов, приёмов, алгоритмов, методов, моделей, критериев и показателей для решения задач по теме занятия.

3. Обсудить и проанализировать основные подходы к решению задач по теме занятия.

4. Попрактиковаться в грамотной постановке задач, учитывающих особенности комплексной защиты объектов информатизации, соотносящихся с изучаемой дисциплиной, с учётом основных требований выпускающей кафедры “Комплексная защита информации”.

Тема 8 (2 ч.). Элементы теории конечных автоматов и понятие об автоматной модели системы защиты GM (проверка сформированности компетенций –ПК-11)

Задания:

1. Выяснить ключевые особенности, подходы, приёмы, алгоритмы, методы, модели, критерии и показатели для решения задач по теме занятия, оформив в виде таблиц для каждого случая.

2. Сделать доклад(ы) по теме занятия.

3. Членам группы научиться грамотно задавать вопросы докладчикам по теме выступления.

4. Выявить в ходе обсуждения основные достоинства и недостатки изложенного докладчиками материала.

5. Предложить свои рекомендации по устранению недостатков изложенного с позиций комплексной защиты объектов информатизации.

Тема 8.2 (2 ч.). Оптимизационная задача о назначениях и разбиение на классы для объектов доступа и субъектов доступа (проверка сформированности компетенций – ПК-11)

Задания:

1. Выяснить ключевые особенности, подходы, приёмы, алгоритмы, методы, модели, критерии и показатели для решения задач по теме занятия, оформив в виде таблиц для каждого случая.

2. Сделать доклад(ы) по теме занятия.

3. Членам группы научиться грамотно задавать вопросы докладчикам по теме выступления.

4. Выявить в ходе обсуждения основные достоинства и недостатки изложенного докладчиками материала.

5. Предложить свои рекомендации по устранению недостатков изложенного с позиций комплексной защиты объектов информатизации.

Тема 9 (2 ч.). Представления о расширенной модели безопасности Take-Grant(проверка сформированности компетенций – ПК-11)

Задания:

1. Выяснить ключевые особенности, подходы, приёмы, алгоритмы, методы, модели, критерии и показатели для решения задач по теме занятия, оформив в виде таблиц для каждого случая.

2. Сделать доклад(ы) по теме занятия.

3. Членам группы научиться грамотно задавать вопросы докладчикам по теме выступления.

4. Выявить в ходе обсуждения основные достоинства и недостатки изложенного докладчиками материала.

5. Предложить свои рекомендации по устранению недостатков изложенного с позиций комплексной защиты объектов информатизации.

Тема 10 (4 ч.). Модель безопасности информационных потоков и другие модели безопасности (проверка сформированности компетенций – ПК-11)

Задания:

1. Выяснить ключевые особенности, подходы, приёмы, алгоритмы, способы, критерии и показатели для решения задач по теме занятия, оформив в виде таблиц для каждого случая.

2. Оценить границы применимости основных подходов, приёмов, алгоритмов, методов, моделей, критериев и показателей для решения задач по теме занятия.

3. Обсудить и проанализировать основные подходы к решению задач по теме занятия.

4. Попрактиковаться в грамотной постановке задач, учитывающих особенности комплексной защиты объектов информатизации, соотносящихся с изучаемой дисциплиной, с учётом основных требований выпускающей кафедры “Комплексная защита информации”.

Тема 11 (4 ч.). Модели контроля целостности информации и контроль доступа, базирующийся на ролях (проверка сформированности компетенций – ПК-11)

Задания:

1. Выяснить ключевые особенности, подходы, приёмы, алгоритмы, способы, критерии и показатели для решения задач по теме занятия, оформив в виде таблиц для каждого случая.

2. Оценить границы применимости основных подходов, приёмов, алгоритмов, методов, моделей, критериев и показателей для решения задач по теме занятия.

3. Обсудить и проанализировать основные подходы к решению задач по теме занятия.

4. Попрактиковаться в грамотной постановке задач, учитывающих особенности комплексной защиты объектов информатизации, соотносящихся с изучаемой дисциплиной, с учётом основных требований выпускающей кафедры “Комплексная защита информации”.

Тема 12 (2 ч.). Расчётные соотношения для контролируемой и неконтролируемой преград комплексной защиты информации (проверка сформированности компетенций –ПК-11)

Задания:

1. Выяснить ключевые особенности, подходы, приёмы, алгоритмы, способы, критерии и показатели для решения задач по теме занятия, оформив в виде таблиц для каждого случая.

2. Оценить границы применимости основных подходов, приёмов, алгоритмов, методов, моделей, критериев и показателей для решения задач по теме занятия.

3. Обсудить и проанализировать основные подходы к решению задач по теме занятия.

4. Попрактиковаться в грамотной постановке задач, учитывающих особенности комплексной защиты объектов информатизации, соотносящихся с изучаемой дисциплиной, с учётом основных требований выпускающей кафедры “Комплексная защита информации”.

Тема 13 (2 ч.). Понятие о сложностных классах задач в ракурсе защиты компьютерной информации (проверка сформированности компетенций – ПК-11)

Задания:

1. Выяснить ключевые особенности, подходы, приёмы, алгоритмы, способы, критерии и показатели для решения задач по теме занятия, оформив в виде таблиц для каждого случая.

2. Оценить границы применимости основных подходов, приёмов, алгоритмов, критериев и показателей для решения задач по теме занятия.

3. Обсудить и проанализировать основные подходы к решению задач по теме занятия.

4. Попрактиковаться в грамотной постановке задач, учитывающих особенности комплексной защиты объектов информатизации, соотносящихся с изучаемой дисциплиной, с учётом основных требований выпускающей кафедры “Комплексная защита информации”.

9.2 Методические рекомендации по подготовке письменных работ

Рекомендуется выполнять письменные работы на листах А-4 от руки либо на компьютере (набор формул на компьютере не обязателен, но писать весь текст следует разборчивым

почерком). Оформляется титульный лист, выполненная работа с титульным листом вкладывается в файл и в назначенный день сдается на проверку преподавателю.

К выполнению заданий для самостоятельной работы предъявляются следующие требования: задания должны исполняться самостоятельно и представляться в установленный срок, а также соответствовать установленным требованиям по оформлению.

Студентам следует:

- руководствоваться графиком самостоятельной работы, определенным РПД;
- выполнять все плановые задания, выдаваемые преподавателем для самостоятельного выполнения, и разбирать на практических занятиях и консультациях неясные вопросы;
- при подготовке к зачёту параллельно прорабатывать соответствующие теоретические и практические разделы дисциплины, фиксируя неясные моменты для их обсуждения на плановой консультации.

Методические рекомендации по подготовке научного доклада. Одной из форм самостоятельной работы студента является подготовка научного доклада, для обсуждения его на практическом занятии.

Цель научного доклада – развитие у студентов навыков аналитической работы с научной литературой, анализа дискуссионных научных позиций, аргументации собственных взглядов. Подготовка научных докладов также развивает творческий потенциал студентов.

Научный доклад готовится под руководством преподавателя, который ведет практические занятия.

Рекомендации студенту:

- перед началом работы по написанию научного доклада согласовать с преподавателем тему, структуру, литературу, а также обсудить ключевые вопросы, которые следует раскрыть в докладе;
- представить доклад научному руководителю в письменной форме;
- выступить на практическом занятии с 10-минутной презентацией своего научного доклада, ответить на вопросы студентов группы.

Требования:

- к оформлению научного доклада: шрифт – TimesNewRoman, размер шрифта – 14, межстрочный интервал 1,5, размер полей – 2,5 см, отступ в начале абзаца – 1,25 см, форматирование по ширине); листы скреплены скоросшивателем. На титульном листе указывается наименование учебного заведения, название кафедры, наименование дисциплины, тема доклада, ФИО студента;
- к структуре доклада – оглавление, введение (указывается актуальность, цель и задачи), основная часть, выводы автора, список литературы (не менее 5 позиций). Объем согласовывается с преподавателем. В конце работы ставится дата ее выполнения и подпись студента, выполнившего работу.

Общая оценка за доклад учитывает содержание доклада, его презентацию, а также ответы на вопросы преподавателя и других слушателей.

9.3 Методические рекомендации по изучению дисциплины

Студентам необходимо прежде всего ознакомиться с содержанием рабочей программы дисциплины (далее – РПД), с целями и задачами дисциплины, ее связями с другими дисциплинами образовательной программы, методическими разработками по данной дисциплине, имеющимися на образовательном портале и сайте кафедры, с графиком консультаций преподавателей данной кафедры.

- *“Сценарий” изучения дисциплины* студентом подразумевает выполнение им следующих действий:

1. Ознакомление с целями и задачами дисциплины.
2. Ознакомление с требованиями к знаниям и навыкам студента.

3. Первичное ознакомление с разделами и темами дисциплины.
4. Ознакомление с распределением времени на изучение дисциплины.
5. Ознакомление со списками рекомендуемой основной и дополнительной литературы по дисциплине.
6. Углублённое ознакомление с разделами и темами дисциплины.
7. Предварительный охват на основе рекомендуемой литературы круга вопросов, актуальных для конкретного занятия.
8. Самостоятельная проработка основного круга вопросов как каждого последующего, так и каждого предыдущего занятия в свободное время между занятиями по дисциплине.
9. Присутствие и творческое участие на лекционных и практических занятиях.
10. Выполнение требований текущего и итогового контроля.
11. Уточнение возникающих вопросов на консультации по дисциплине.
12. Непосредственная подготовка к зачёту по дисциплине.

Рекомендации по работе с литературой. Целесообразно пользоваться литературой, изданной не более 7 лет назад, предшествовавших году начала изучения курса. В вопросах дискретной математики, непосредственно касающихся программной реализации решаемых в курсе задач на ЭВМ, используемая литература должна быть по возможности ещё более новой – как правило, 5–6 летней давности издания.

Рекомендации по подготовке к занятиям. Изучение дисциплины требует систематического и последовательного накопления знаний, следовательно, пропуски отдельных тем не позволяют глубоко освоить предмет. Именно поэтому контроль над систематической работой студентов всегда находится в центре внимания кафедры.

Студентам необходимо:

- перед каждой лекцией просматривать рабочую программу дисциплины, что позволит сэкономить время на записывание темы лекции, ее основных вопросов, рекомендуемой литературы;

- на отдельные лекции приносить соответствующий материал на бумажных носителях, представленный лектором на портале или присланный на «электронный почтовый ящик группы» (таблицы, графики, схемы). Данный материал будет охарактеризован, прокомментирован, дополнен непосредственно на лекции;

- перед очередной лекцией необходимо просмотреть по конспекту материал предыдущей лекции. При затруднениях в восприятии материала следует обратиться к основным литературным источникам, если разобраться в материале опять не удалось, то обратитесь к лектору (по графику его консультаций) или к преподавателю на практических занятиях. Не следует оставлять «белых пятен» в освоении материала.

Студентам также следует:

- до очередного практического занятия по рекомендованным литературным источникам проработать теоретический материал соответствующей темы занятия;

- при подготовке к практическим занятиям следует обязательно использовать не только лекции, но и учебную литературу,

- в начале занятий задать преподавателю вопросы по материалу, вызвавшему затруднения в его понимании и освоении при решении задач, заданных для самостоятельного решения;

- в ходе практического занятия давать конкретные, четкие ответы по существу вопросов;

- на занятии доводить каждую задачу до окончательного решения, демонстрировать понимание проведенных расчетов (анализов, ситуаций), в случае затруднений обращаться к преподавателю.

Студентам, пропустившим занятия (независимо от причин), не имеющие письменного решения задач или не подготовившиеся к данному практическому занятию, рекомендуется не позже чем в 2-недельный срок явиться на консультацию к преподавателю и отчитаться по теме, изучавшейся на занятии. Студенты, не отчитавшиеся по каждой не проработанной ими на заня-

тиях теме к началу зачетной сессии, упускают возможность получить положенные баллы за работу в соответствующем семестре.

Методические рекомендации по работе с литературой. Любая форма самостоятельной работы студента (подготовка к практическому занятию, написание эссе, курсовой работы, доклада и т.п.) начинается с изучения соответствующей литературы как в библиотеке, так и дома.

Рекомендации студенту:

- выбранную монографию или статью целесообразно внимательно просмотреть. В книгах следует ознакомиться с оглавлением и научно-справочным аппаратом, прочитать аннотацию и предисловие. Целесообразно ее пролистать, рассмотреть иллюстрации, таблицы, диаграммы, приложения. Такое поверхностное ознакомление позволит узнать, какие главы следует читать внимательно, а какие – прочитать быстро;
- в книге или журнале, принадлежащие самому студенту, ключевые позиции можно выделять маркером или делать пометки на полях. При работе с Интернет-источником целесообразно также выделять важную информацию;
- если книга или журнал являются собственностью студента, то целесообразно записывать номера страниц, которые привлекли внимание. Позже следует возвратиться к ним, перечитать или переписать нужную информацию. Физическое действие по записыванию помогает прочно заложить данную информацию в «банк памяти».

Записи в той или иной форме не только способствуют пониманию и усвоению изучаемого материала, но и помогают вырабатывать навыки явного изложения в письменной форме тех или иных теоретических вопросов.

Приложение 1. Аннотация
рабочей программы дисциплины

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Дисциплина «Математические основы защиты информации» реализуется на факультете Информационных систем и безопасности кафедрой комплексной защиты информации.

Цель дисциплины: обучение студентов основным принципам и подходам к использованию математического аппарата для криптографической и комплексной защиты информации.

Задачи дисциплины:

- научить определять и учитывать качественные и количественные особенности составляющих криптографической и комплексной защиты информации;
- сформировать у студентов представления о механизмах смены параметров криптографической защиты;
- научить решать основополагающие теоретико-практические задачи защиты информации с применением необходимого математического аппарата и сформировать математический подход к их решению;
- ознакомить студентов с математическими основами криптографических методов защиты компьютерной информации;
- ознакомить студентов с основными математическими принципами алгоритмов создания электронной цифровой подписи;
- ознакомить студентов с основными принципами построения систем комплексной защиты информации.

Дисциплина направлена на формирование следующих компетенций:

- ПК-11 – Способен применять положения криптографии, теории алгоритмов, комплексной защиты информации при решении прикладных задач

В результате освоения дисциплины обучающийся должен:
Знать: основные понятия, методы, принципы, подходы, алгоритмы и приёмы криптографии и комплексной защиты информации;
Уметь: применять основные методы, принципы, подходы, алгоритмы и приёмы криптографии и комплексной защиты информации с необходимыми формулами для решения профессиональных математических задач;
Владеть: основными подходами к постановке и решению задач, навыками математического описания профессиональных прикладных задач.

По дисциплине предусмотрена промежуточная аттестация в форме *зачёта*.
Общая трудоёмкость дисциплины составляет 3 зачётные единицы.