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

ОСНОВЫ КРИПТОГРАФИИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Направление подготовки 01.03.04 Прикладная математика
Направленность (профиль) Математика информационных сред
Уровень квалификации выпускника – бакалавр
Форма обучения – очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2021

ОСНОВЫ КРИПТОГРАФИИ
Рабочая программа дисциплины

Составитель:
Кандидат технических наук, доцент, доцент кафедры комплексной защиты информации РГГУ, доцент кафедры международной информационной безопасности ФГБОУ ВО МГЛУ М.В. Шептунов

Ответственный редактор
Кандидат технических наук, и.о. зав. кафедрой комплексной защиты информации
Д.А. Митюшин

УТВЕРЖДЕНО
Протокол заседания кафедры
комплексной защиты информации
№ 13 от 29.06.2021 г.

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины – получение основных представлений об использовании криптографических методов, базирующихся на алгебре и теории чисел, для защиты хранимой информации и при дистанционной передаче электронных документов.
Задачи дисциплины:
- преподать студентам базовые математические понятия криптографии для овладения ими, в т.ч., для изучения последующих профильных дисциплин;
- научить студентов решать типовые задачи дисциплины;
- научить студентов использовать математический аппарат для решения теоретических и прикладных задач дисциплины.

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

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ОПК-2. Способен обоснованно выбирать, дорабатывать и применять для решения исследовательских и проектных задач математические методы и модели, осуществлять проверку адекватности моделей, анализировать результаты, оценивать надежность и качество функционирования систем	ОПК-2.3. Планомерно следует определенной логике, ведущей к решению текущей задачи.	*Знать:* • криптологическую терминологию; • основные теоремы теории чисел, используемые в криптографии; • основные теоретико-числовые алгоритмы; • основные алгоритмы, реализующие арифметические операции в основных алгебраических структурах, используемых в криптографических приложениях; • основные требования к взаимосвязанным математическим параметрам в криптосистемах. *Уметь:* • применять математический аппарат для решения поставленных задач. *Владеть:* • навыками работы с алгоритмами криптоанализа асимметричных криптосистем в ракурсе задачи факторизации.
ОПК-4. Способен разрабатывать алгоритмы и компьютерные программы, пригодные для практического применения	ОПК-4.2. Анализирует области применимости возникающих задач практической деятельности	*Знать:* • криптологическую терминологию; • основные теоремы теории чисел, используемые в криптографии; • основные теоретико-числовые алгоритмы; • основные алгоритмы, реализующие арифметические операции в основных алгебраических структурах, используемых в криптографических приложениях; • основные требования к взаимосвязанным математическим параметрам в

		криптосистемах и их математическим моделям. *Уметь:* • применять математический аппарат для решения поставленных задач *Владеть:* • навыками работы с алгоритмами криптоанализа асимметричных криптосистем в ракурсе задачи факторизации

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Основы криптографии» относится к обязательной части блока дисциплин учебного плана.
Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин: Линейная алгебра, Теория графов, Теория вероятностей, Дискретная математика.
В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения прохождения практик: Научно-исследовательская работа.

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет 2 з.е., 76 ч., в том числе контактная работа обучающихся с преподавателем 28 ч., самостоятельная работа обучающихся 48 ч.

№ п/п	Раздел дисциплины	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
			Контактная				Промежуточная аттестация	Самостоятель-ная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия			
1	Раздел I. Некоторые исторические шифры и смежные вопросы: одноключевые криптосистемы	8	4		8			10	Устный опрос, 1-й тест, доклады
2	Раздел II. Математические элементы криптографии и разделения секрета	8	4		6			14	Устный опрос, 2-й тест, контрольная (аудиторная самостоятельная) работа, доклады
3	Раздел III. Основные пути совершенствования существующих шифров	8	2		2			8	Устный опрос, доклады
4	Зачёт	8			2			16	Зачёт по билетам
	итого:		**10**		**18**			**48**	

3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1	**Раздел I. Некоторые исторические шифры и смежные вопросы: одноключевые криптосистемы**	***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
2	**Раздел II. Математические элементы криптографии и разделения секрета**	***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. 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 ***Тема 5. 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 6. 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
3	**Раздел III. Основные пути совершенствования существующих шифров**	***Тема 7. Основные разновидности атак на шифры – криптоанализа*** Дифференциальный криптоанализ. Дифференциальный криптоанализ на основе отказов устройства. Линейный криптоанализ. Некоторые другие виды криптоанализа и атак. ***Тема 8. Некоторые современные подходы к шифрованию информации*** Возможности шифрования на основе метода укладки рюкзака (упаковки ранца). Криптосхема с перестановкой фиксированных процедур. Шифры на основе процедур и операций преобразования, зависящих от преобразуемых данных. Шифры: с управляемыми операциями, на основе управляемых перестановок, с управляемыми подстановками, на основе модифицирования подключей.

4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	**2**	**3**	**4**
1.	Некоторые исторические шифры и смежные вопросы: одноключевые криптосистемы	Лекция 1. Основы одноключевых криптосистем	Вводная лекция – теоретическая справка с кратким изложением основных понятий
		Практическое занятие 1. Основы одноключевых криптосистем	Вводное занятие. Решение задач у доски с обсуждением. Дискуссия.
		Самостоятельная работа	Консультирование посредством электронной почты.
		Лекция 2. Аналитический метод шифрования	Лекция с разбором конкретных ситуаций.
		Практическое занятие 2. Аналитический метод шифрования	Решение задач у доски с обсуждением. Дискуссия.
		Самостоятельная работа	Консультирование посредством электронной почты.
2.	Математические элементы криптографии и разделения секрета	Лекция 3. Обратимость и теоретико-числовые основы криптографии.	Лекция с разбором конкретных ситуаций.
		Практическое занятие 3. Обратимость и теоретико-числовые основы криптографии	Решение задач у доски с обсуждением. Дискуссия.
		Самостоятельная работа	Консультирование посредством электронной почты.
		Лекция 4. Понятие о схемах разделения секрета и (древне)китайская теорема об остатках.	Теоретическая справка с кратким изложением основных понятий и решением задач.
		Практическое занятие 4. Понятие о схемах разделения секрета и (древне)китайская теорема об остатках.	Дискуссия.

		Самостоятельная работа	Консультирование посредством электронной почты.
		Лекция 5. Основы двухключевых криптосистем	Лекция с использованием частично-поисковых методов обучения.
		Практическое занятие 5. Основы двухключевых криптосистем	Самостоятельное моделирование задач с последующим их обсуждением и оптимизацией. Дискуссия.
		Самостоятельная работа	Консультирование посредством электронной почты.
		Лекция 6. Алгоритм RSA и его использование в режиме шифрования	Развернутая беседа с обсуждением доклада Лекция с использованием частично-поисковых методов обучения.
		Практическое занятие 6. Алгоритм RSA и его использование в режиме шифрования	Семинар с использованием частично-поисковых методов обучения.
		Самостоятельная работа	Консультирование посредством электронной почты.
3.	Основные пути совершенствования существующих шифров	Лекция 7. Основные разновидности атак на шифры – криптоанализа	Лекция с использованием частично-поисковых методов обучения.
		Практическое занятие 7. Основные разновидности атак на шифры – криптоанализа	Самостоятельное моделирование задач с последующим их обсуждением и оптимизацией. Дискуссия.
		Самостоятельная работа	Консультирование посредством электронной почты.
		Лекция 8. Некоторые современные подходы к	Лекция с использованием частично-поисковых

		шифрованию информации Практическое занятие 8. Некоторые современные подходы к шифрованию информации Самостоятельная работа	методов обучения. Семинар с использованием частично-поисковых методов обучения. Дискуссия. Консультирование и проверка домашних заданий посредством электронной почты.

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	*11 баллов*	*22 балла*
- аудиторная самостоятельная либо контрольная работа (домашняя либо аудиторная)	*22 балла*	*22 балла*
- посещаемость теоретических и практических занятий	*3 балла (за каждую половину семестра)*	*6 баллов*
- работа в аудитории (в том числе, устные опросы и творческая активность на занятиях, с учётом работы у доски и с места, качества и количества ответов)	*3 балла (за каждую половину семестра)*	*6 баллов*
- занятие призовых мест на олимпиадах и конкурсах, наличие публикаций (тезисов конференций, статей, в том числе, в соавторстве) по математическому либо смежному профилю	*4 балла*	*4 балла*
Промежуточная аттестация *(зачёт по билетам)*		*40 баллов*
Итого за дисциплину *зачёт*		*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».
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.

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения 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

Текущий контроль

Примерные вопросы Теста №1

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.
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.
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.
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.
5. При совместном восстановлении ключа:
A) всем участникам схемы разделения секрета необходимо собраться в одном помещении;
B) всем участникам схемы разделения секрета необходимо собраться в одном здании;
C) части участников схемы разделения секрета необходимо собраться в одном помещении;
D) ничего из перечисленного.
6. Существует ли понятие “тени” защищаемого схемой разделения секрета ключа:
A) да; B) нет; C) постановка вопроса некорректна; D) существует синоним это понятия.
7. 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.
8. 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.
9. Число r в схеме разделения секрета, основанной на древнекитайской теореме об остатках:
A) необходимо знать только одному (любому) из легальных участников;
B) необходимо знать всегда двум легальным участникам;
C) необходимо знать всегда только центру распределения ключей;
D) ничего из перечисленного.
10. В используемых в основанной на древнекитайской теореме об остатках схеме разделения секрета выражениях $(N_1 \cdot M_1) \pmod{m_1} \equiv 1$ и $(N_2 \cdot M_2) \pmod{m_2} \equiv 1$ числа N_1 и N_2:

A) могут совпасть; B) не могут и не должны совпадать; C) обычно никак не используются; D) всегда одинаковы.

Примерные вопросы Теста №2

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. Криптосистема (алгоритм) RSA может использоваться:

A) только в режиме шифрования;
B) только в режиме электронной цифровой подписи;
C) как в режиме шифрования, так и в режиме электронной цифровой подписи;
D) при одном ключе как в режиме шифрования, так и в режиме электронной цифровой подписи.
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) отсутствует;
B) существует;
C) существует и её размерность всегда 3x3 или 2x2;
D) существует и обычно она квадратная.
7. Может ли в шифре на основе маршрутов Гамильтона взаимное расположение и взаимосвязи между вершинами неорграфа-таблицы и орграфов-маршрутов отличаться:
A) да; B) нет; C) иногда; D) постановка вопроса некорректна, т. к. в этом методе шифрования нет всех перечисленных особенностей.
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. Верно следующее:
A) числа p и q взаимно просты тогда и только тогда, когда выполнено соотношение up-vq=1 для некоторых целых чисел u, v;
B) числа p и q взаимно просты тогда и только тогда, когда выполнено соотношение up-vq=1 для всех целых чисел u, v;
C) требуется дополнительное исследование;
D) постановка как первого, так и второго вопроса некорректна.
10. В методе шифрования на основе маршрутов Гамильтона:
A) они всегда замкнуты; B) они иногда замкнуты; C) они иногда разомкнуты;
D) они обычно разомкнуты.

Примерные задания контрольной (самостоятельной аудиторной) работы
(вариант выбирается по последней цифре (либо соответственно двум последним цифрам) цифрам студенческого билета – зачётной книжки)

1. Применяя алгоритм RSA, зашифровать и расшифровать сообщение.

i	0	1	2	3	4	5	6	7	8	9
Текст	ВОДА	ДЕВА	БИЧ	СЫЧ	СЫР	БАК	КРАБ	КРАН	ГИД	ИМЯ
j	0	1	2	3	4	5	6	7	8	9
p либо *q*	7	11	3	5	13	7	17	11	5	13

Примечание. В задании №1 вариант задания определяется 2-мя последними цифрами номера зачётной книжки. Из данной табл. по предпоследней i выбирается шифруемый текст (сообщение), а по последней j – одно из чисел (p либо q), требуемых для реализации алгоритма.

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

Вариант	0	1	2	3	4	5	6	7	8	9
Ключ K	20	21	22	23	24	25	16	17	18	19

3. 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	0	1	2	3	4	5	6	7	8	9
a	19	4	10	10	9	31	181	10	17	35
m	93	7	13	7	11	73	19	11	13	82

4. Зашифровать и расшифровать сообщение методом матричной алгебры (аналитический метод шифрования).

i =1: ПОБЕДА; i =2: КОЛОСС; i =3: КАБИНА; i =4: ДОПУСК; i =5: СЕКРЕТ;
i =6: КРАЙНЕ; i =7: КНИЖКА; i =8: ВОЗДУХ; i =9: ПОДЪЁМ; i =0: ЛЖИВЫЙ;

$$j\text{=}1\text{:}\ A=\begin{pmatrix}1&6&8\\3&9&7\\4&7&1\end{pmatrix};\quad j\text{=}2\text{:}\ A=\begin{pmatrix}2&6&8\\3&9&7\\4&7&2\end{pmatrix};\quad j\text{=}3\text{:}\ A=\begin{pmatrix}3&6&8\\3&9&7\\4&7&3\end{pmatrix};\quad j\text{=}4\text{:}\ A=\begin{pmatrix}4&6&8\\3&9&7\\4&7&4\end{pmatrix};$$

$$j\text{=}5\text{:}\ A=\begin{pmatrix}5&6&8\\3&9&7\\4&7&5\end{pmatrix};\quad j\text{=}6\text{:}\ A=\begin{pmatrix}6&6&8\\3&9&7\\4&7&6\end{pmatrix};\quad j\text{=}7\text{:}\ A=\begin{pmatrix}7&6&8\\3&9&7\\4&7&7\end{pmatrix};\quad j\text{=}8\text{:}\ A=\begin{pmatrix}8&6&8\\3&9&7\\4&7&8\end{pmatrix};$$

$$j\text{=}9\text{:}\ A=\begin{pmatrix}9&6&8\\3&9&7\\4&7&9\end{pmatrix};\quad j\text{=}0\text{:}\ A=\begin{pmatrix}6&9&1\\3&9&7\\5&7&9\end{pmatrix}.$$

Пояснения к выбору варианта – по соответственно одной последней либо двум последним цифрам номера зачётной книжки либо студенческого билета;
для задания 4 (на шифрование и расшифрование методом матричной алгебры) по предпоследней цифре i выбирается шифруемое сообщение (слово), а по последней j – матрица-ключ A.

Примерная тематика докладов

1. Конечные поля Галуа и возможности их применения в задачах компьютерной безопасности и схемах разделения секрета.

2. Возможности конечных автоматов при математическом описании различных шифров.

3. Возможности конечных автоматов при математическом описании различных кодов.

4. Перспективы и трудности применения автоматной модели системы защиты GM в криптографической защите информации.

5. Возможности применения модели Low-Water-Mark в системах криптографической защиты информации.

6. Модель Биба и возможности её использования при контроле целостности криптографически защищённой информации.

7. Модель Кларка-Вилсона и возможности её использования при контроле целостности криптографически защищённой информации.

Промежуточная аттестация

При проведении *промежуточной аттестации* студент должен выполнить 8 заданий билета письменного зачёта (4 тестовых задания, 2 вопроса теоретического характера и 2 практического характера).

Примерные контрольные вопросы

1. Понятие ключа шифрования, принцип (правило) Кёркхоффа и его применение к одноключевым криптосистемам.
2. Алгоритм Евклида и его применение.
3. Обратимость как важное свойство, используемое в криптографии. Вычисление обратных величин. Расширенный алгоритм Евклида и его применение.
4. Основы одноключевых криптосистем.
5. Шифр Трисемуса и шифр Гронсфельда, примеры.
6. Шифр Гронсфельда и алгоритм RSA.
7. Шифр "двойной квадрат" Уитстона и шифр Гронсфельда, примеры.
8. Шифр Вижинера и шифр Гронсфельда.
9. Матричный (аналитический) метод шифрования-дешифрования.
10. Асимметричные криптосистемы.
11. Криптосистема (алгоритм) RSA.
12. Функция Эйлера и её применение в криптосистеме (алгоритме) RSA.
13. Задача факторизации и криптосистема (алгоритм) RSA.
14. (Древне)китайская теорема об остатках и возможности её использования в целях защиты информации.
15. Операция mod и её использование в криптографии.
16. Вычисление обратных величин.
17. Отличие между криптосистемой и схемой разделения секрета, примеры.
18. Односторонняя функция, заложенная в основу криптосистемы RSA.
19. Схема разделения секрета на основе (древне)китайской теоремы об остатках.
20. Понятия кольца, вычета, поля Галуа.
21. Шифрование маршрутами Гамильтона.
22. Решение систем сравнений.
23. 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.

Примерные практические задания

1. Используя схему разделения секрета, основанную на (древне)китайской теореме об остатках, защитить общий для двух компаньонов ключ *K=19*. (При отыскании *N* из выражений вида $(N \cdot M)(\mathrm{mod}\, m) = 1$ применить два способа – поочерёдная проверка значений, расширенный алгоритм Евклида).

2. Применяя алгоритм RSA, зашифровать и расшифровать сообщение ИМЯ при заданном *p* либо *q*: 13.

3. Применяя расширенный алгоритм Евклида, найти обратный элемент a^{-1} по модулю *m=82* для *a=35* (при условии его существования) и проверить, что найденные числа *u, v* удовлетворяют равенству $au + mv = 1$.

4. Зашифровать и расшифровать сообщение "МЕНЬШЕ" методом матричной алгебры с заданной матрицей-ключом $A = \begin{pmatrix} 1 & 6 & 8 \\ 3 & 9 & 7 \\ 4 & 7 & 1 \end{pmatrix}$.

Примерные вопросы для тестирования

001. Из современных подходов к шифрованию информации могут применяться:
-методы укладки рюкзака (упаковки ранца);
криптосхема с перестановкой фиксированных процедур;
-шифры на основе управляемых перестановок;
-шифры с управляемыми подстановками;
-шифры на основе модифицирования подключей;
-ничего из перечисленного.
002. Бывают шифры:
-простой замены;
-сложной замены;
-перестановки;
-основанные на трудности решения задачи факторизации;
-ничего из перечисленного.
003. Метод шифрования маршрутами Гамильтона:
-характеризуется тем, что в нём длина каждого блока обязательно равна 4;
-характеризуется тем, что в нём длина каждого блока обязательно равна 3;
-характеризуется тем, что в нём используется таблица;
-характеризуется тем, что в нём в любом случае бессмысленно использовать неорграф-таблицу, а применяются только орграфы.
004. Понятие матрицы-ключа:
-отсутствует;
-существует;
-существует и её размерность только 3x3 или 2x2;
-существует и она только единичная.
005. Верно следующее:
-числа p и q взаимно просты тогда и только тогда, когда выполнено соотношение up-vq=1 для некоторых целых чисел u, v;
-числа p и q взаимно просты тогда и только тогда, когда выполнено соотношение up-vq=1 для всех целых чисел u, v;
-требуется дополнительное исследование;

-постановка как первого, так и второго вопроса некорректна.
006. В методе шифрования на основе маршрутов Гамильтона:
-они должны быть замкнуты;
-они только периодически замкнуты;
-они, как правило, должны быть разомкнуты;
-постановка вопроса некорректна.
007. Схема разделения секрета называется совершенной:
-если легальное либо нелегальное множество участников полностью раскрывает секрет;
-если произвольное множество участников либо полностью раскрывает секрет, либо в результате получает о нём минимум информации;
-только если произвольное множество двух либо более участников в результате своих действий не получает о секрете информацию;
-ничего из перечисленного.
008. Более криптостойким (в общем случае) является шифр (криптосистема):
-Гронсфельда в сопоставлении с шифром Вижинера;
-Вижинера в сопоставлении с шифром Гронсфельда;
-“двойной квадрат” Уитстона в сопоставлении с шифром Гронсфельда;
-шифр Гронсфельда в сопоставлении с шифром “двойной квадрат” Уитстона.
009. В пороговых схемах разделения секрета:
-обязательно полный состав участников должен объединить свои усилия для совместного получения доступа к объекту защиты;
-обязательно большинство участников должны объединить свои усилия для совместного получения доступа к объекту защиты;
-обязательно меньшинство участников должны объединить свои усилия для совместного получения доступа к объекту защиты;
-ничего из перечисленного.
010. Могут ли в шифре на основе маршрутов Гамильтона взаимное расположение и взаимосвязи между вершинами неорграфа-таблицы и орграфов-маршрутов отличаться:
-да;
-нет;
-постановка вопроса некорректна, т.к. в этом методе шифрования нет всех перечисленных особенностей;
-ничего из перечисленного?
011. Древнекитайскую теорему об остатках:
-нельзя использовать в схеме разделения секрета, если количество участников более 2-х;
-можно использовать в схеме разделения секрета, если количество участников более 2-х;
-можно использовать исключительно для разделения секрета;
-ничего из перечисленного.
012. Гамильтонов маршрут и гамильтонов цикл применительно к шифрованию:
-одно и то же;
-близкие, но отличающиеся понятия;
-требуется дополнительное исследование;
-постановка вопроса некорректна.
013. В общем случае криптоалгоритм RSA:
-работает быстрее одноключевых криптоалгоритмов;
-работает медленнее одноключевых криптоалгоритмов;
-работает с той же скоростью, что и одноключевые криптоалгоритмы;
-ничего из перечисленного.
014. Центр распределения ключей:
-в любом случае нежелательно использовать при разделении секрета;
-как правило, не используют при разделении секрета;

-используют исключительно тогда, когда разделение секрета происходит на основе древнекитайской теоремы об остатках;
-ничего из перечисленного.
015. В аналитическом (матричном) методе шифрования:
-один ключ;
-несколько ключей, каждый из которых – элемент матрицы-ключа;
-нет ни одного ключа;
-два ключа.
016. При совместном восстановлении ключа:
-полному составу участников схемы разделения секрета необходимо собраться в одном помещении;
-полному составу участников схемы разделения секрета необходимо собраться в одном здании;
-части участников схемы разделения секрета необходимо собраться в одном помещении;
-ничего из перечисленного.
017. Существует ли понятие “тени” защищаемого схемой разделения секрета ключа:
-да;
-нет;
-постановка вопроса некорректна;
-существует синоним это понятия.
018. Возможны схемы разделения секрета:
-основанные только на древнекитайской теореме об остатках, ибо другие так и не созданы;
-основанные на любых теоремах;
-геометрической природы;
-с количеством участников как менее 10, так и более 10.
019. Обязательно ли в схемах разделения секрета у каждого из участников одинаковые доли секрета:
-да;
-нет;
-зависит только от значения числового ключа;
-постановка вопроса некорректна?
020. Криптосистема (алгоритм) RSA может использоваться:
-только в режиме шифрования;
-только в режиме электронной цифровой подписи;
-либо в режиме шифрования, либо в режиме электронной цифровой подписи;
-ничего из перечисленного.
021. В шифре “двойной квадрат” Уитстона обе таблицы:
-могут быть только прямоугольными, но никак не квадратными;
-могут быть только квадратными;
-могут иметь различающееся между 1-й и 2-й таблицами количество строк;
-ничего из перечисленного.
022. В системе шифрования Вижинера длина ключа:
-не может превышать 4;
- равна 4;
-может превышать 4;
-нулевая.

Демонстрационный вариант билета для зачёта **№0**

1. Сравнения, как и обычные целые числа:
A) можно только складывать; B) можно только умножать; C) можно складывать и умножать;

D) ничего из перечисленного, поскольку постановка вопроса некорректна. (***до 4 баллов***)
2. Корректна ли запись $m_1 m_2 \equiv m \equiv 0 (\mathrm{mod}\, m)$:
A) да;
B) нет;
C) да, только если бы в ней отсутствовал 0;
D) да, только если бы в ней вместо 0 была 1? (***до 4 баллов***)
3. Шифрование с помощью таблиц Трисемуса является:
A) монограммным; B) биграммным; C) зависит только от размеров таблицы;
D) ничего из перечисленного. (***до 4 баллов***)
4. 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. (***до 4 баллов***)
5. Обратимость как важное свойство, используемое в криптографии. Вычисление обратных величин. Расширенный алгоритм Евклида и его применение. (***до 5 баллов***)

6. Шифр Трисемуса и шифр Гронсфельда, примеры. (***до 5 баллов***)

7. Используя схему разделения секрета, основанную на (древне)китайской теореме об остатках, защитить общий для двух компаньонов ключ *K=18*. (При отыскании *N* из выражений вида $(N \cdot M)(\mathrm{mod}\, m) = 1$ рекомендуется применить любые два из трёх изучавшихся способов – поочерёдная проверка значений, вычисление на основе функции Эйлера при использовании алгоритма быстрого возведения в степень, расширенный алгоритм Евклида). (***до 7 баллов***)

8. Применяя алгоритм RSA, зашифровать и расшифровать сообщение ГИД при заданном *p* либо *q*: 5. (***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. Защита информации : учеб. пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - Москва : РИОР : ИНФРА-М, 2018. - 392 с. - (Высшее образование: Бакалавриат; Магистратура). — https://doi.org/10.12737/4868. - ISBN 978-5-369-01378-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/937469. – Режим доступа: по подписке.

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. Перечень современных профессиональных баз данных (БД) и информационно-справочных систем (ИСС)

№ п/п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2020 г. Web of Science Scopus
2	Компьютерные справочные правовые системы Консультант Плюс, Гарант

7. Материально-техническое обеспечение дисциплины

Для материально-технического обеспечения дисциплины необходимы:

- учебная аудитория,
- доска,
- проектор (стационарный или переносной),
- компьютер или ноутбук,
- программное обеспечение (ПО).

Перечень программного обеспечения (ПО)

№ п/п	Наименование ПО	Производитель	Способ распространения (*лицензионное или свободно распространяемое*)
1	Microsoft Office 2010 Pro	Microsoft	лицензионное
2	Windows XP/ Windows 7 / Windows 10	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное
4	Zoom	Zoom	лицензионное

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 расчеты;
- развитие инициативы и самостоятельности студентов;
- формирование навыков публичного выступления, способности представлять результаты проведенного 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 - определенный 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. Основы одноключевых криптосистем

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 раздела I.

Тема 2. Аналитический метод шифрования

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 (например, задействуя двукратное шифрование на основе изученного метода).

Тема 3. Обратимость и теоретико-числовые основы криптографии

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.

Тема 4. Понятие о схемах разделения секрета и (древне)китайская теорема об остатках

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.

Тема 5. Основы двухключевых криптосистем

Задания:

1. Выяснить ключевые особенности, подходы, приёмы, алгоритм, модель, показатели для решения задач по теме занятия, оформив в виде таблиц для каждого случая.

2. Оценить границы применимости основных подходов, приёмов, алгоритма, моделей, 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.

Тема 6. Алгоритм RSA и его использование в режиме шифрования

Задания:

1. Выяснить ключевые особенности, подходы, приёмы, алгоритм, 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 и прикладной математики.

Тема 7. Основные разновидности атак на шифры – криптоанализа

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.

Тема 8. Некоторые современные подходы к шифрованию информации

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 и прикладной математики.

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 – Times New Roman, 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 занятиях 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.

ПРИЛОЖЕНИЯ

Приложение 1

АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Основы криптографии» реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации.

Цель дисциплины: получение основных представлений об использовании криптографических методов, базирующихся на алгебре и теории чисел, для защиты хранимой информации и при дистанционной передаче электронных документов.
Задачи:
- преподать студентам базовые математические понятия криптографии для овладения ими, в т.ч., для изучения последующих профильных дисциплин;
- научить студентов решать типовые задачи дисциплины;
- научить студентов использовать математический аппарат для решения теоретических и прикладных задач дисциплины.

Дисциплина направлена на формирование следующих компетенций:

- ОПК-2. Способен обоснованно выбирать, дорабатывать и применять для решения исследовательских и проектных задач математические методы и модели, осуществлять проверку адекватности моделей, анализировать результаты, оценивать надежность и качество функционирования систем.
- ОПК-4. Способен разрабатывать алгоритмы и компьютерные программы, пригодные для практического применения.

В результате освоения дисциплины обучающийся должен:
Знать: криптологическую терминологию; основные теоремы теории чисел, используемые в криптографии; основные теоретико-числовые алгоритмы; основные алгоритмы, реализующие арифметические операции в основных алгебраических структурах, используемых в криптографических приложениях; основные требования к взаимосвязанным математическим параметрам в криптосистемах.
Уметь: применять математический аппарат для решения поставленных задач.
Владеть: навыками работы с алгоритмами криптоанализа асимметричных криптосистем в ракурсе задачи факторизации.

По дисциплине предусмотрена промежуточная аттестация в форме зачета.

Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы.

Приложение 2

ЛИСТ ИЗМЕНЕНИЙ

№	Текст актуализации или прилагаемый к РПД документ, содержащий изменения	Дата	№ протокола
1	Приложение к листу изменений №1		