Федеральное государственное бюджетное образовательное учреждение инклюзивного высшего образования

«Московский государственный гуманитарно-экономический университет»

Факультет Прикладной математики и информатики

Кафедра Информационных технологий и прикладной математики

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 041CD9B1001CAF77894D606F5F479EB1E9
Владелец: Сахарчук Елена Сергеевна
Действителен: с 26.09.2022 до 26.09.2023

УТВЕРЖДАЮ

И.о. Проректора по учебно-методической работе
Хакимов Р.М.

_____
«____»_____ 2021г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ) КРИПТОГРАФИЯ

образовательная программа направления подготовки
01.03.02 "Прикладная математика и информатика"
Б1.В.ДВ.05.01 «Дисциплины (модули)», часть, формируемая участниками образовательных отношений, дисциплины (модули) по выбору

Профиль подготовки
Вычислительная математика и информационные технологии

Квалификация (степень) выпускника:
Бакалавр

Форма обучения: очная

Курс 4 семестр 8

Москва
2021

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования по направлению подготовки 01.03.02 «Прикладная математика и информатика (уровень бакалавриата)», утвержденного приказом Министерства образования и науки Российской Федерации № 9 от 10 января 2018 г. Зарегистрировано в Минюсте России 06 февраля 2018 г. №49937.

Составители рабочей программы: МГГЭУ, доцент кафедры Информационных технологий и прикладной математики
место работы, занимаемая должность

подпись Петрунина Е.В. «30» августа 2021 г.
Ф.И.О. Дата

Рецензент: МГГЭУ, профессор кафедры Информационных технологий и прикладной математики
место работы, занимаемая должность

подпись Истомина Т.В. «30» августа 2021 г.
Ф.И.О. Дата

Рабочая программа утверждена на заседании кафедры Информационных технологий и прикладной математики (протокол № 2 от «30» августа 2021 г.)

Зав. кафедрой ИТиПМ_ подпись Митрофанов Е.П. «30» августа 2021 г.
Ф.И.О. Дата

СОГЛАСОВАНО
Начальник
учебного отдела
«30» августа 2021 г. подпись И.Г.Дмитриева
Дата Ф.И.О.

СОГЛАСОВАНО
Декан факультета ПМиИ
«30» августа 2021 г. подпись Е.В. Петрунина
Дата Ф.И.О.

СОГЛАСОВАНО
Заведующая библиотекой
«30» августа 2021 г. подпись В.А. Ахтырская
Дата Ф.И.О.

1. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

1.1. Цель и задачи изучения учебной дисциплины (модуля)

Дисциплина предполагает формирование у студентов знаний по проблеме криптографической защиты информационных ресурсов, а также практических навыков безопасной работы в информационных системах.

1.2. Требования к результатам освоения дисциплины

Изучение данной дисциплины направлено на формирование следующих компетенций:

Код и содержание компетенции	**Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций**
ПК-7. Способен к разработке и применению алгоритмических и программных решений в области системного и прикладного программного обеспечения	ПК-7.1. Знает теоретические основы разработки программных и алгоритмических решений в области системного и прикладного программного обеспечения; математические методы решения задач, процедурный и объектно-ориентированный подходы к разработке информационных систем; актуальные проблемы в области программирования; методы и технологии программирования; языки программирования, основы технологии модульного программирования на языках высокого уровня.
	ПК-7.2. Умеет применить математический метод для решения задачи; подобрать рациональную технологию программирования для решения профессиональной задачи; создавать программные продукты и алгоритмические решения в области системного и прикладного программного обеспечения.
	ПК-7.3. Владеет навыками применения математических методов для решения задач и применения стандартных алгоритмов; навыками разработки и создания алгоритмических и программных решений в области системного и прикладного программного обеспечения; навыками разработки программных приложений с использованием современных языков программирования.

1.3. Место дисциплины (модуля) в структуре образовательной программы направления подготовки 01.03.02 «Прикладная математика и информатика»

Учебная дисциплина «Криптография» относится к части, формируемой участниками образовательных отношений блока Б1. Изучение учебной дисциплины «Криптография» базируется на знаниях, умениях и навыках, полученных обучающимися при изучении дисциплин «Информационная безопасность», «Объектно-ориентированное программирование», «Системное и прикладное программное обеспечение».

Изучение учебной дисциплины «Криптография» необходимо для выполнения выпускной квалификационной работы.

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Объем дисциплины и виды учебной работы в соответствии с формами обучения

Объем дисциплины «Криптография» составляет 3 зачетных единицы/108 часов:

Вид учебной работы	Всего, часов	Очная форма
		Курс, часов
		4 курс
		8 сем.
Аудиторная работа обучающихся с преподавателем (по видам учебных занятий), всего в том числе:	*36*	*36*
Лекции	12	12
Практические занятия	24	24
Лабораторные занятия		
Самостоятельная работа обучающихся	36	36
Промежуточная аттестация (подготовка и сдача), всего:		
Контрольная работа		
Курсовая работа		
Зачет		
Экзамен	36	36
Итого: Общая трудоемкость учебной дисциплины (в часах, зачетных единицах)	108/3	108/3

2.2. Содержание дисциплины по темам (разделам)

№ п/п	Наименование раздела (темы)	Содержание раздела (тематика занятий)	Формируемые компетенции (индекс)
1.	**Тема 1.** Введение в криптографию	Основные понятия, термины, определения. Предмет и задачи дисциплины. Из истории криптографии. Простейшие шифры и их свойства. Шифры замены и перестановки. Композиции шифров. Основные этапы становления криптографии как науки. Характер криптографической деятельности. Открытые сообщения и их характеристики. Виды информации, подлежащие закрытию, их модели и свойства. Частотные характеристики открытых сообщений. Критерии на открытый текст. Особенности нетекстовых сообщений. Основные понятия криптографии. Модели шифров. Блочные и поточные шифры. Понятие криптосистемы. Ручные и машинные шифры. Ключевая система шифра. Основные требования к шифрам.	ПК-7
2.	**Тема 2.** Шифры перестановки.	Разновидности шифров перестановки: маршрутные, вертикальные перестановки, решетки и лабиринты. Криптоанализ шифров перестановки. Шифры замены. Одноалфавитные и многоалфавитные замены. Вопросы криптоанализа простейших шифров замены. Стандартные алгоритмы	ПК-7

		криптографической защиты данных. Современные системы шифрования (симметрические и асимметрические). Поточные шифры. Табличное и модульное гаммирование. Случайные и псевдослучайные гаммы. Криптограммы, полученные при повторном использовании ключа. Анализ криптограмм, полученных применением неравновероятной гаммы. Синтез и анализ криптографических алгоритмов: классические шифры, шифры гаммирования и колонной замены.	
3.	**Тема 3.** Теория К.Шеннона	Теоретико-информационный подход к оценке криптостойкости шифров. Криптографическая стойкость шифров. Надежность ключей и сообщений. Совершенные шифры. Безусловно стойкие и вычислительно стойкие шифры. Вопросы практической стойкости. Избыточность языка и расстояние единственности	ПК-7
4.	**Тема 4.** Имитостойкость шифров	Имитация и подмена сообщения. Характеристики имитостойкости. Методы обеспечения имитостойкости шифров. Совершенная имитостойкость. Коды аутентификации. Основные методы дешифрования. Помехоустойчивость шифров. Характеристики помехоустойчивости. Характеризация шифров, не размножающих искажений типа замены и пропуска букв.	ПК-7
5.	**Тема 5.** Реализация криптографических алгоритмов	Основные способы реализация криптографических алгоритмов и требования, предъявляемые к ним. Различие между программными и аппаратными реализациями. Программные реализации шифров. Программно-аппаратная реализация современных криптографических схем и систем. Особенности использования вычислительной техники в криптографии. Современные криптографические интерфейсы. Криптографические стандарты. Стандарты систем шифрования (DES, ГОСТ 28147-89). Вопросы синтеза шифров.	ПК-7
6.	**Тема 6.** Модели криптографических протоколов	Сложность криптографических алгоритмов (теорема Кука, np-полнота). Криптографические протоколы, протоколы с нулевым разглашением. Основные примеры. Связь стойкости протокола со стойкостью базовой криптографической системы. Классификация криптографических протоколов. Электронная цифровая подпись (ЭЦП). Понятие ЭЦП. Стандарты ЭЦП. Однонаправленные функции и методы их построения.	ПК-7

2.3. Разделы дисциплин и виды занятий

№ п/п	Наименование темы дисциплины	Лекционные занятия	Практические занятия	Самостоятельная работа	Всего часов	Формы текущего контроля успеваемости
1.	Введение в криптографию	2	4	6	12	Устный опрос
2.	Шифры перестановки	2	4	6	12	Устный опрос
3.	Теория К.Шеннона	2	4	6	12	Устный опрос
4.	Имитостойкость шифров	2	4	6	12	Устный опрос
5.	Реализация криптографических алгоритмов	2	4	6	12	Устный опрос
6.	Модели криптографических протоколов	2	4	6	12	Устный опрос
Экзамен		**36**				
	Итого:	12	24	36	108	

2.4. Планы теоретических (лекционных) занятий

№	Наименование тем лекций	Кол-во часов в семестре
8 семестр		
ТЕМА 1. Введение в криптографию.		
1.	Простейшие шифры и их свойства. Шифры замены и перестановки. Композиции шифров. Характер криптографической деятельности.	2
ТЕМА 2. Шифры перестановки.		
1.	Разновидности шифров перестановки: маршрутные, вертикальные перестановки, решетки и лабиринты. Криптоанализ шифров перестановки. Шифры замены. Одноалфавитные и многоалфавитные замены.	2
ТЕМА 3. Теория К.Шеннона.		
1.	Теоретико-информационный подход к оценке криптостойкости шифров.	2
ТЕМА 4. Имитостойкость шифров.		
1.	Имитация и подмена сообщения. Характеристики имитостойкости. Методы обеспечения имитостойкости шифров.	2
ТЕМА 5. Реализация криптографических алгоритмов.		
1.	Основные способы реализация криптографических алгоритмов и требования, предъявляемые к ним. Различие между программными и аппаратными реализациями.	2
ТЕМА 6. Модели криптографических протоколов.		
1.	Сложность криптографических алгоритмов (теорема Кука, np-полнота). Классификация криптографических протоколов.	2

2.5. Планы практических (семинарских) занятий

№	Наименование практических занятий	Кол-во часов в семестре
8 семестр		
ТЕМА 1. Введение в криптографию.		
1.	Открытые сообщения и их характеристики. Виды информации, подлежащие закрытию, их модели и свойства. Частотные характеристики открытых сообщений.	2

2.	Критерии на открытый текст. Особенности нетекстовых сообщений. Основные понятия криптографии. Модели шифров. Блочные и поточные шифры..	2
ТЕМА 2. Шифры перестановки.		
1.	Стандартные алгоритмы криптографической защиты данных. Современные системы шифрования. Поточные шифры. Табличное и модульное гаммирование.	2
2.	Случайные и псевдослучайные гаммы. Криптограммы, полученные при повторном использовании ключа. Анализ криптограмм, полученных применением неравновероятной гаммы	2
ТЕМА 3. Теория К.Шеннона.		
1.	Криптографическая стойкость шифров. Надежность ключей и сообщений.	2
2.	Совершенные шифры. Безусловно стойкие и вычислительно стойкие шифры.	2
ТЕМА 4. Имитостойкость шифров.		
1.	Совершенная имитостойкость. Коды аутентификации. Основные методы дешифрования.	2
2.	Помехоустойчивость шифров. Характеристики помехоустойчивости.	2
ТЕМА 5. Реализация криптографических алгоритмов.		
1.	Программные реализации шифров. Программно-аппаратная реализация современных криптографических схем и систем.	2
2.	Особенности использования вычислительной техники в криптографии. Современные криптографические интерфейсы и стандарты.	2
ТЕМА 6. Модели криптографических протоколов.		
1.	Криптографические протоколы, протоколы с нулевым разглашением. Основные примеры.	2
2.	Связь стойкости протокола со стойкостью базовой криптографической системы. Электронная цифровая подпись (ЭЦП).	2

2.6. Планы лабораторных работ – не предусмотрено.

2.7. Планы самостоятельной работы обучающегося по дисциплине (модулю).

№	Название разделов и тем	Виды самостоятельной работы	Трудоемкость	Формируемые компетенции	Формы контроля
1.	Введение в криптографию	Понятие криптосистемы. Ручные и машинные шифры. Ключевая система шифра. Основные требования к шифрам.	6	ПК-7	Устный опрос
2.	Шифры перестановки	Синтез и анализ криптографических алгоритмов: классические шифры, шифры гаммирования и колонной замены.	6	ПК-7	Устный опрос
3.	Теория К.Шеннона	Вопросы практической стойкости. Избыточность языка и расстояние единственности.	6	ПК-7	Устный опрос
4.	Имитостойкость шифров	Характеризация шифров, не размножающих искажений типа замены и пропуска букв.	6	ПК-7	Устный опрос

5.	Реализация криптографических алгоритмов	Стандарты систем шифрования (DES, ГОСТ 28147-89). Вопросы синтеза шифров.	6	ПК-7	Устный опрос
6.	Модели криптографических протоколов	Стандарты ЭЦП. Однонаправленные функции и методы их построения.	6	ПК-7	Устный опрос

3. ОСОБЕННОСТИ ОБУЧЕНИЯ ЛИЦ С ИНВАЛИДНОСТЬЮ И ОВЗ

Обучение лиц с ограниченными возможностями здоровья осуществляется с учетом индивидуальных психофизических особенностей, а для инвалидов также в соответствии с индивидуальной программой реабилитации инвалида.

Для получения обучающимися, имеющими ограниченные физические возможности, качественного образования должны выполняться следующие важные условия: обучающийся должен иметь возможность беспрепятственно посещать образовательное учреждение и использовать в своём обучении дистанционные образовательные технологии.

Для обучения и контроля обучающихся с нарушениями координации движений предусмотрено проведение тестирования с использованием компьютера.

Во время аудиторных занятий обязательно использование средств обеспечения наглядности учебного материала с помощью мультимедийного проектора. Скорость изложения материала должна учитывать ограниченные физические возможности студентов.

4. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение дисциплины для организации самостоятельной работы студентов (содержит перечень основной литературы, дополнительной литературы, программного обеспечения и Интернет-ресурсы).

В распоряжении преподавателей и обучающихся имеется основное необходимое материально-техническое оборудование, Интернет-ресурсы, доступ к полнотекстовым электронным базам, книжный фонд библиотеки Московского государственного гуманитарно-экономического университета.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Перечень основной литературы

1. Криптографическая защита информации : учебное пособие / С. О. Крамаров, О. Ю. Митясова, С. В. Соколов [и др.] ; под ред. С. О. Крамарова. — Москва : РИОР : ИНФРА-М, 2021. — 321 с. — (Высшее образование). - ISBN 978-5-369-01716-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1153156
2. Бабаш, А. В. История защиты информации в зарубежных странах : учебное пособие / А.В. Бабаш, Д.А. Ларин. — Москва : РИОР : ИНФРА-М, 2021. — 284 с. — (Высшее образование). — DOI: https://doi.org/10.12737/15090. - ISBN 978-5-369-01844-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1215133
3. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2021. — 400 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1210523

4. Романьков, В. А. Введение в криптографию : курс лекций / В.А. Романьков. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 240 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-00091-493-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1514566

5.2 Перечень дополнительной литературы

1. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2021. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/469567

2. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2021. — 245 с. — (Высшее образование). — ISBN 978-5-9916-7090-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/470279

3. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2021. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/469758

5.3 Программное обеспечение

1. Сетевой компьютерный класс, оснащенный современной техникой
2. Офисный программный пакет (например, Microsoft Office 2003 или более поздних версий).
3. Web-браузер Mozilla Firefox или Google Chrome
4. Экран для проектора

5.4 Электронные ресурсы

1. Электронная библиотека «Знаниум»: https://znanium.com/
2. Электронная библиотека «Юрайт»: https://urait.ru/
3. Научная электронная библиотека «Elibrary.ru»: https://www.elibrary.ru/defaultx.asp

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий	Перечень оборудования и технических средств обучения
1.	Лекционная аудитория	Персональный компьютер, мультимедийный проектор
2.	Компьютерный класс	Персональные компьютеры (IBM PC-совместимые) под управлением ОС Microsoft Windows, компьютерная сеть, доступ в сеть Интернет

7. ОЦЕНКА КОМПЕТЕНЦИЙ ПО ИЗУЧАЕМОЙ ДИСЦИПЛИНЕ

№	Критерии оценки			
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
	ЗНАТЬ			
1	Студент не способен самостоятельно выделять главные положения в изученном материале дисциплины. Не знает теоретических основ разработки программных и алгоритмических решений в области системного и прикладного программного обеспечения; математических методов решения задач, процедурного и объектно-ориентированного подходов к разработке информационных систем.	Студент усвоил основное содержание материала дисциплины, но имеет пробелы в усвоении материала. Имеет несистематизированные знания о теоретических основах разработки программных и алгоритмических решений в области системного и прикладного программного обеспечения.	Студент способен самостоятельно выделять главные положения в изученном материале. Знает теоретические основы разработки программных и алгоритмических решений в области системного и прикладного программного обеспечения; математические методы решения задач.	Студент знает, понимает, выделяет главные положения в изученном материале и способен дать краткую характеристику основным идеям проработанного материала дисциплины. Показывает глубокое знание и понимание теоретических основ разработки программных и алгоритмических решений в области системного и прикладного программного обеспечения; математических методов решения задач, процедурного и объектно-ориентированного подходов к разработке информационных систем.
	УМЕТЬ			
2	Студент не умеет осуществлять применять математический метод для решения задачи; подбирать рациональную технологию программирования для решения профессиональной задачи; создавать программные продукты и алгоритмические решения в области системного и	Студент испытывает затруднения при применении математического метода для решения задачи. Студент непоследовательно подбирает рациональную технологию программирования для решения профессиональной задачи.	Студент умеет самостоятельно применить математический метод для решения задачи; подобрать рациональную технологию программирования для решения профессиональной задачи.	Студент умеет самостоятельно применить математический метод для решения задачи; подобрать рациональную технологию программирования для решения профессиональной задачи; создавать программные продукты и алгоритмические

	прикладного программного обеспечения.			решения в области системного и прикладного программного обеспечения.
ВЛАДЕТЬ				
3	Студент не владеет навыками применения математических методов для решения задач и применения стандартных алгоритмов; навыками разработки и создания алгоритмических и программных решений в области системного и прикладного программного обеспечения.	Студент владеет базовыми навыками применения математических методов для решения задач и применения стандартных алгоритмов	Студент владеет навыками применения математических методов для решения задач и применения стандартных алгоритмов; навыками разработки и создания алгоритмических и программных решений в области системного и прикладного программного обеспечения.	Студент владеет знаниями всего изученного материала, владеет навыками применения математических методов для решения задач и применения стандартных алгоритмов; навыками разработки и создания алгоритмических и программных решений в области системного и прикладного программного обеспечения.
	Компетенции или их части не сформированы	Компетенции или их части сформированы на базовом уровне	Компетенции или их части сформированы на среднем уровне	Компетенции или их части сформированы на высоком уровне

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Интерактивные образовательные технологии, используемые в аудиторных занятиях и самостоятельной работе обучающихся – не предусмотрены.

9. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

9.1. Организация входного, текущего и промежуточного контроля обучения

Входное тестирование – не предусмотрено.
Текущий контроль – устный опрос.
Промежуточная аттестация – экзамен.

9.2. Тематика рефератов, проектов, творческих заданий, эссе и т.п.

Не предусмотрены.

9.3. Курсовая работа

Не предусмотрено.

9.4. Вопросы к зачету

Не предусмотрены.

9.5. Вопросы к экзамену

1. Симметричное шифрование. Принцип Керкгофса.
2. Примеры применения криптографии. Классы атак.
3. Подстановочный шифр и его взлом.
4. Шифр Виженера, роторная машина.
5. Определение шифра. Шифр Вернама и совершенная секретность.
6. Вероятностные переформулировки совершенной секретности.
7. Эксперимент по взлому. Длина ключа в случае совершенной секретности.
8. Псевдослучайный генератор и его предсказуемость. Линейный конгруэнтный генератор.
9. Атаки на потоковые шифры.
10. Статистические тесты, преимущество. Надежность псевдослучайного генератора.
11. Непредсказуемость надежного генератора. Вычислительная неразличимость.
12. Определение схемы шифрования с закрытым ключом. Вычислительная стойкость.
13. Стойкость потокового шифра. Шифрование нескольких сообщений.
14. Стойкость относительно chosen plaintext-атак. Функции с ключом и псевдослучайные функции.
15. Шифрование с помощью псевдослучайной функции и его устойчивость.
16. Псевдослучайные перестановки. Методы работы блочных шифров.
17. Конструкции псевдослучайных перестановок. Сеть Фейстеля.
18. Аутентификация сообщений. Код аутентификации сообщений и его надежность.
19. Конструкция кода аутентификации сообщений из псевдослучайной функции.
20. Протокол интерактивного обмена ключами, его надежность. Описание протокола Диффи–Хеллмана.
21. Задача DDH и надежность протокола Диффи–Хеллмана.
22. Схема шифрования с открытым ключом, ее надежность относительно подслушивания и относительно chosen plaintext-атак.
23. Шифрование нескольких сообщений, его надежность. Гибридное шифрование.
24. Наивная схема шифрования RSA. Ускорение дешифровки, маленький показатель.
25. RSA с набивкой, задача RSA и надежность схемы шифрования RSA с набивкой.
26. Схема Эль-Гамаля и ее надежность.
27. Квадратичные вычеты и символ Якоби.

28. Задача определения квадратичных вычетов и схема шифрования Гольдвассер–Микали.
29. Извлечение квадратных корней и схема шифрования Рабина.
30. Остатки по модулю N2 и схема шифрования Пайе.
31. Схема цифровой подписи, ее надежность. Наивная схема RSA.
32. RSA с хэшем. Схема одноразовой подписи Лэмпорта.
33. Доказательства с нулевым разглашением.
34. Сертификаты. Схемы разделения секрета.

9.6. Контроль освоения компетенций

Вид контроля	**Контролируемые темы (разделы)**	**Компетенции, компоненты которых контролируются**
Устный опрос	*1,2,3,4,5,6*	*ПК-7*

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Номер и дата протокола заседания кафедры	Перечень измененных пунктов	Подпись заведующего кафедрой