

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		



**УТВЕРЖДЕНО**

решением Ученого совета факультета математики, информационных и авиационных технологий

от « 18 » 05 2021 г., протокол № 4/21

Председатель М.А. Волков

(подпись, расшифровка подписи)

« 18 » 05 2021 г.

**РАБОЧАЯ ПРОГРАММА**

Дисциплина	Дополнительные главы криптографии
Факультет	Математики, информационных и авиационных технологий
Кафедра	Информационной безопасности и теории управления
Курс	5

Специальность: 10.05.01 «Компьютерная безопасность»

*код направления (специальности), полное наименование*

Специализация: «Математические методы защиты информации»

*полное наименование*

Форма обучения: очная

*очная, заочная, очно-заочная (указать только те, которые реализуются)*

Дата введения в учебный процесс УлГУ: « 01 » 09 2021 г.

Программа актуализирована на заседании кафедры: протокол № \_\_\_\_\_ от \_\_\_\_\_ 20\_\_\_\_ г.

Программа актуализирована на заседании кафедры: протокол № \_\_\_\_\_ от \_\_\_\_\_ 20\_\_\_\_ г.

Программа актуализирована на заседании кафедры: протокол № \_\_\_\_\_ от \_\_\_\_\_ 20\_\_\_\_ г.

Сведения о разработчиках:

ФИО	Кафедра	Должность, ученая степень, звание
Рацев Сергей Михайлович	ИБиТУ	профессор, д.ф-м.н, доцент

СОГЛАСОВАНО	СОГЛАСОВАНО
Заведующий кафедрой «Информационная безопасность и теория управления», реализующей дисциплину	Заведующий выпускающей кафедрой «Информационная безопасность и теория управления»
 / Андреев А.С. / (подпись) (Ф.И.О.)	 / Андреев А.С. / (подпись) (Ф.И.О.)
« 12 » 05 2021 г.	« 12 » 05 2021 г.

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

## 1. ЦЕЛИ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

### Цель освоения дисциплины:

- развитие навыка построения постквантовых криптографических протоколов.

### Задачи освоения дисциплины:

- овладение основными идеями и методами построения постквантовых криптографических систем;
- формирование навыков грамотного применения теоретических основ криптографии в постановке практических задач, в решении задач с применением современного теоретического аппарата, в систематизации полученных знаний.

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к факультативным дисциплинам (ФТД) образовательной программы и читается в 9-м семестре студентам специальности «Компьютерная безопасность» очной формы обучения.

Для успешного освоения дисциплины необходимы знания основных фактов из базовых курсов: «Алгебра», «Дискретная математика», «Методы и средства криптографической защиты информации», «Информатика».

Для освоения дисциплины студент должен иметь следующие «входные» знания, умения, навыки и компетенции: основные задачи и понятия криптографии; классификацию шифров по различным признакам; типы основных способов криптоанализа шифров; основные типы электронной подписи.

Дисциплина «Криптографические протоколы» является предшествующей для прохождения практики и итоговой государственной аттестации.

## 3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СОТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины «Дополнительные главы криптографии» направлен на формирование следующих компетенций.

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
ПК-3 – Способен разрабатывать проектные решения по защите информации в компьютерных системах	Знать: основные виды симметричных и асимметричных криптографических алгоритмов; математические модели шифров; Уметь: корректно применять симметричные и асимметричные криптографические алгоритмы; Владеть: криптографической терминологией;
ПК-5 – Способен участвовать в разработке программных и программно-аппаратных средств для систем защиты информации компьютерных систем	Знать: основные виды симметричных и асимметричных криптографических алгоритмов; математические модели шифров; Уметь: корректно применять симметричные и асимметричные криптографические алгоритмы

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

Владеть: криптографической терминологией;
--

#### 4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего) 3.

4.2. Объем дисциплины по видам учебной работы:

Вид учебной работы	Количество часов (форма обучения - дневная)			
	Всего по плану	В т.ч. по семестрам		
		9		
Контактная работа обучающихся с преподавателем	36/36*	36/36*		
Аудиторные занятия:	36/36*	36/36*		
• Лекции	18/18*	18/18*		
• Практические и семинарские занятия				
• Лабораторные работы (лабораторный практикум)	18/18*	18/18*		
Самостоятельная работа	36	36		
Форма текущего контроля знаний и контроля самостоятельной работы				
Всего часов по дисциплине	72	72		
Виды промежуточного контроля (экзамен, зачет)	Зачет	Зачет		
Общая трудоемкость в зач. ед.	2	2		

\*В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий в таблице через слеш указывается количество часов работы ППС с обучающимися для проведения занятий в дистанционном формате с применением электронного обучения

4.3. Содержание дисциплины. Распределение часов по темам и видам учебной работы:

Форма обучения очная

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерак-	Самостоя-	
		Лекции	Практические	Лабораторные			

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

			занятия, семина- ры	работы, практи- кумы	тивной форме	тельная работа	
1	2	3	4	5	6	7	
1. Криптогра- фия, основанная на хеш- функциях.	8	4				4	
2. Алгоритмы декодирования алгебраических кодов.	24	4		8	4	12	Домашние за- дания.
3. Криптогра- фия, основанная на кодах исправ- ления ошибок.	32	6		10	8	16	Домашние за- дания. лабора- торные работы
4. Криптогра- фия, основанная на решётках.	8	4				4	
Итого:	72	18		18	12	36	

## 5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

### Тема 1. Криптография, основанная на хеш-функциях.

Основные требования, которым должна удовлетворять хеш-функция. Построение хеш-функций. Задачи, решаемые с помощью электронных подписей. Надежность электронной подписи. Электронная подпись на основе схем одноразовой подписи; представление подписи как пути в дереве связанных хеш-значений. Стойкость схемы сводится к предположению о стойкости используемой хеш-функции относительно задач поиска коллизий и/или прообразов. Древоподобная подпись Меркля.

### Тема 2. Алгоритмы декодирования алгебраических кодов.

Алгоритм Берлекэмп-Мессе над любым полем. Алгоритм Берлекэмп-Мессе над двоичным полем. Алгоритм Берлекэмп-Мессе с минимальным числом вычислений обратных элементов. Обобщенный алгоритм Евклида. Взаимосвязь алгоритма Берлекэмп-Мессе и обобщенного алгоритма Евклида. Криптоанализ последовательности, выработанной с помощью регистра сдвига с линейной обратной связью, на основе алгоритма Берлекэмп-Мессе. Декодирование алгебраических кодов на основе алгоритма Берлекэмп-Мессе. Алгоритм декодирования Сугиямы.

### Тема 3. Криптография, основанная на кодах исправления ошибок.

Обобщенные коды Рида-Соломона. Альтернативные коды. Коды Гоппы. Построение проверочной матрицы кода Гоппы. Двоичные коды Гоппы. Примеры двоичных кодов Гоппы. Классическая и модернизированная криптосистемы Мак-Элиса. Классическая и модернизированная криптосистемы Нидеррайтера. Современная кодовая криптосистема на основе кодов Гоппы.

### Тема 4. Криптография, основанная на решётках.

Задача поиска кратчайшего вектора (SVP); SVP 2 NP. Задача поиска ближайшего вектора (CVP); CVP 2 NP. Обучение с ошибками (LWE; RLWE). Наименьшее целочисленное решение СЛАУ (SIS). Система Ring-Learning with Errors.

## 6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

Практические (семинарские) занятия не предусмотрены учебным планом.

## 7. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)

Полные задания для лабораторных работ приводятся в учебно-методическом пособии: Аминаров А. В. Лабораторный практикум по математическим методам защиты информации : учеб.-метод. указания для спец. "Компьютерная безопасность, "Математическое обеспечение и администрирование информационных систем" / А. В. Аминаров, А. М. Иванцов, С. М. Рацеев. Ульяновск : УлГУ, 2016. 55 с.

Лабораторные работы проводятся в интерактивной форме, а именно, используются: диалоговое обучение, в ходе которого осуществляется взаимодействие между студентом и преподавателем, между самими студентами, группами студентов; элементы деловых игр, «мозговой штурм» или дискуссии по рассматриваемым вопросам.

### Тема 2. Алгоритмы декодирования алгебраических кодов.

Цель работы: освоить методику алгоритмов декодирования.

Задание. Требуется реализовать алгоритмы декодирования обобщенных кодов Рида-Соломона на основе алгоритма Гао, алгоритма Берлекэмп-Мессис и алгоритма Сугиямы.

Методические указания: основное внимание должно быть уделено освоению принципов декодирования алгебраических кодов.

### Тема 3. Криптография, основанная на кодах исправления ошибок.

Цель работы: освоить методику работы кодов Гоппы.

Задание. Требуется реализовать код Гоппы.

Методические указания: основное внимание должно быть уделено освоению принципов построения кодов Гоппы.

### Тема 3. Криптография, основанная на кодах исправления ошибок.

Цель работы: изучение постквантовых протоколов.

Задание. Реализовать криптосистему Мак-Элиса на основе кодов Гоппы.

Методические указания: основное внимание должно быть уделено освоению постквантовых протоколов.

## 8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

Курсовые и контрольные работы не предусмотрены учебным планом дисциплины.

## 9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ

1. Электронная подпись на основе схем одноразовой подписи.
2. Представление подписи как пути в дереве связанных хеш-значений.
3. Древовидная подпись Меркля.
4. Обобщенные коды Рида-Соломона.
5. Алгоритм Берлекэмп-Мессис.
6. Альтернативные коды.
7. Коды Гоппы.
8. Построение проверочной матрицы кода Гоппы.
9. Двоичные коды Гоппы.
10. Примеры двоичных кодов Гоппы.
11. Схема шифрования McEliece на основе кодов Гоппы.
12. Схемы шифрования Niederreiter на основе кодов Гоппы.
13. Задача поиска кратчайшего вектора (SVP); SVP 2 NP.
14. Задача поиска ближайшего вектора (CVP); CVP 2 NP.
15. Обучение с ошибками (LWE; RLWE).
16. Наименьшее целочисленное решение СЛАУ (SIS).

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

### 10. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

Название разделов и тем	Вид самостоятельной работы	Объем в часах	Форма контроля
1. Криптография, основанная на хэш-функциях.	Проработка учебного материала, подготовка к сдаче зачета	4	Зачет
2. Алгоритмы декодирования алгебраических кодов.	Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета	12	Зачет, проверка лабораторных работ
3. Криптография, основанная на кодах исправления ошибок.	Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета	16	Зачет, проверка лабораторных работ
4. Криптография, основанная на решётках.	Проработка учебного материала, подготовка к сдаче зачета	4	Зачет

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

## 11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### а) Список рекомендуемой литературы

#### основная

1. Васильева И.Н. Криптографические методы защиты информации : учебник и практикум для академического бакалавриата / И. Н. Васильева. Москва : Издательство Юрайт, 2019. 349 с. (Серия : Бакалавр. Академический курс). ISBN 978-5-534-02883-6. Текст : электронный // ЭБС Юрайт [сайт]. URL: <https://biblio-online.ru/bcode/433610>
2. Рацеев С.М. Математические методы защиты информации : электронный учебный курс / С. М. Рацеев; УлГУ, ФМИАТ. - Ульяновск : УлГУ, 2018. — URL: <http://edu.ulsu.ru/courses/921/interface>

#### дополнительная

1. Поднебесова Г.Б. Абстрактная и компьютерная алгебра [Электронный ресурс]: практикум/ Поднебесова Г.Б.— Электрон. текстовые данные.— Челябинск: Южно-Уральский государственный гуманитарно-педагогический университет, 2016.— 125 с.— Режим доступа: <http://www.iprbookshop.ru/83852.html>
2. ГОСТ-Эксперт – единая база ГОСТов Российской Федерации для образования и промышленности:
  - 2.1. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. М.: Стандартинформ, 2012. — URL: <https://gostexpert.ru/gost/gost-34.10-2012>
  - 2.2. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования. М.: Стандартинформ, 2013. — URL: <https://gostexpert.ru/gost/gost-34.11-2012>

#### учебно-методическая

1. Аминаров А. В. Лабораторный практикум по математическим методам защиты информации : учеб.-метод. указания для спец. "Компьютерная безопасность, "Математическое обеспечение и администрирование информационных систем" / А. В. Аминаров, А. М. Иванцов, С. М. Рацеев. Ульяновск : УлГУ, 2016. 55 с. - URL: <http://lib.ulsu.ru/MegaPro/Download/MObject/270>
2. Рацеев С. М. Методические указания для самостоятельной работы студентов по дисциплине «Дополнительные главы криптографии» для студентов специальности 10.05.01 «Компьютерная безопасность» / С. М. Рацеев; УлГУ, Фак. математики, информ. и авиац. технологий. - Ульяновск : УлГУ, 2019. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 145 КБ). - Текст : электронный. Режим доступа: <http://lib.ulsu.ru/MegaPro/Download/MObject/4684>

Согласовано:

П.С.Сиб-рь      И.В. ЧагУ      Помина И.Р      Вел, 04.05.2021  
 должность сотрудника научной библиотеки      ФИО      подпись      дата

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

## б) Программное обеспечение

Для образовательного процесса по данной дисциплине необходим стационарный класс ПК с установленным следующим программным обеспечением:

- операционная среда ОС Windows/Linux;
- системы программирования на языках Си/C++ (Code::Blocks).

## в) Профессиональные базы данных, информационно-справочные системы

### 1. Электронно-библиотечные системы:

1.1. IPRbooks : электронно-библиотечная система : сайт / группа компаний Ай Пи Ар Медиа. - Саратов, [2021]. – URL: <http://www.iprbookshop.ru>. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. ЮРАЙТ : электронно-библиотечная система : сайт / ООО Электронное издательство ЮРАЙТ. – Москва, [2021]. - URL: <https://urait.ru>. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. Консультант студента : электронно-библиотечная система : сайт / ООО Политехресурс. – Москва, [2021]. – URL: <https://www.studentlibrary.ru/cgi-bin/mb4x>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Консультант врача : электронно-библиотечная система : сайт / ООО Высшая школа организации и управления здравоохранением-Комплексный медицинский консалтинг. – Москва, [2021]. – URL: <https://www.rosmedlib.ru>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО Букап. – Томск, [2021]. – URL: <https://www.books-up.ru/ru/library/>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.6. Лань : электронно-библиотечная система : сайт / ООО ЭБС Лань. – Санкт-Петербург, [2021]. – URL: <https://e.lanbook.com>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. **Znanium.com** : электронно-библиотечная система : сайт / ООО Знаниум. - Москва, [2021]. - URL: <http://znanium.com> . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

1.8. Clinical Collection : коллекция для медицинских университетов, клиник, медицинских библиотек // EBSCOhost : [портал]. – URL: <http://web.b.ebscohost.com/ehost/search/advanced?vid=1&sid=9f57a3e1-1191-414b-8763-e97828f9f7e1%40sessionmgr102> . – Режим доступа : для авториз. пользователей. – Текст : электронный.

1.9. Русский язык как иностранный : электронно-образовательный ресурс для иностранных студентов : сайт / ООО Компания «Ай Пи Ар Медиа». – Саратов, [2021]. – URL: <https://ros-edu.ru>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

**2. КонсультантПлюс** [Электронный ресурс]: справочная правовая система. /ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2021].

### 3. Базы данных периодических изданий:

3.1. База данных периодических изданий : электронные журналы / ООО ИВИС. - Москва, [2021]. – URL: <https://dlib.eastview.com/browse/udb/12>. – Режим доступа : для авториз. пользователей. – Текст : электронный.

3.2. eLIBRARY.RU: научная электронная библиотека : сайт / ООО Научная Электронная Библиотека. – Москва, [2021]. – URL: <http://elibrary.ru>. – Режим доступа : для авториз. пользователей. – Текст : электронный

3.3. «Grebennikon» : электронная библиотека / ИД Гребенников. – Москва, [2021]. – URL: <https://id2.action-media.ru/Personal/Products>. – Режим доступа : для авториз. пользователей. – Текст : электронный.

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

**4. Национальная электронная библиотека** : электронная библиотека : федеральная государственная информационная система : сайт / Министерство культуры РФ ; РГБ. – Москва, [2021]. – URL: <https://нэб.рф>. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

**5. SMART Imagebase** // EBSCOhost : [портал]. – URL: <https://ebSCO.smartimagebase.com/?TOKEN=EBSCO-1a2ff8c55aa76d8229047223a7d6dc9c&custid=s6895741>. – Режим доступа : для авториз. пользователей. – Изображение : электронные.

**6. Федеральные информационно-образовательные порталы:**

6.1. Единое окно доступа к образовательным ресурсам : федеральный портал / учредитель ФГАОУ ДПО ЦРГОП и ИТ. – URL: <http://window.edu.ru/>. – Текст : электронный.

6.2. Российское образование : федеральный портал / учредитель ФГАОУ ДПО ЦРГОП и ИТ. – URL: <http://www.edu.ru>. – Текст : электронный.

**7. Образовательные ресурсы УлГУ:**

7.1. Электронная библиотека УлГУ : модуль АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: <http://lib.ulsu.ru/MegaPro/Web>. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

Согласовано:

Зам.нач. УИТиТ  
должность сотрудника УИТиТ

/ Клочкова А.В.  
ФИО

  
подпись

04.05.2021  
дата

