УТВЕРЖДЕНО
решением Ученого совета факультета математики,
информационных и авиационных технологий
от «_17_» ___05_____2022_г., протокол №_4/22_
Председатель _____
(подпись, расшифровка подписи)
«_17_» ____05_____ 2022___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_____ 2022___ г.

Программа актуализирована на заседании кафедры: протокол №_13_ от __11.05.2022___ 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
Рацеев Сергей Михайлович	ИБиТУ	профессор, д.ф-м.н, доцент

СОГЛАСОВАНО:
Заведующий выпускающей кафедрой «Информационная безопасность и теория управления» /_____/ Андреев А.С. / *(подпись) (Ф.И.О.)* «__11__»_____05_____2022___г.

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), СОТНЕСЕНЫХ 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

	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 ин-	Само-	
		Лекции	Практи-	Лабора-			

			ческие занятия, семина-ры	торные работы, практи-кумы	терак-тивной форме	стоя-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. Древовидная подпись Меркля.

Тема 2. Алгоритмы декодирования алгебраических кодов.

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

Тема 3. Криптография, основанная на кодах исправления ошибок.

Обобщенные коды Рида-Соломона. Альтернативные коды. Коды Гоппы. Построение проверочной матрицы года 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

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 Берлекэмпа-Месси 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 Берлекэмпа-Месси.
6. Альтернативные коды.
7. Коды Гоппы.
8. Построение проверочной матрицы года 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).

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

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 : учебное пособие для вузов / С. М. Рацеев. — Санкт-Петербург : Лань, 2022. — 544 с. — ISBN 978-5-8114-8589-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/193323

дополнительная

1. Бабаш А. В. Моделирование системы защиты информации: Практикум : Учебное пособие / Бабаш А. В., Баранова Е. К.; Национальный исследовательский университет "Высшая школа экономики". - 3 ; перераб. и доп. - Москва : Издательский Центр РИОР, 2021. - 320 с. - ВО - Бакалавриат. - Режим доступа: ЭБС Znanium; по подписке. - ISBN 978-5-369-01848-4. - ISBN 978-5-16-108538-7. - ISBN 978-5-16-016214-0. Ссылка на ресурс http://znanium.com/catalog/document?id=371348
2. 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
3. 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 специальностей 10.05.01 «Компьютерная безопасность» и 10.05.03 «Информационная безопасность автоматизированных систем» / С. М. Рацеев. - Ульяновск : УлГУ, 2022. - 9 с. - Неопубликованный ресурс. - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/13329

Согласовано:

ДИРЕКТОР НБ / БУРХАНОВА М.М. / 04.05.2022

Должность сотрудника научной библиотеки — ФИО — подпись — дата

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/С++ (Code::Blocks).

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. Цифровой образовательный ресурс IPRsmart : электронно-библиотечная система : сайт / ООО Компания «Ай Пи Ар Медиа». - Саратов, [2022]. – URL: http://www.iprbookshop.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. Образовательная платформа ЮРАЙТ : образовательный ресурс, электронная библиотека : сайт / ООО Электронное издательство ЮРАЙТ. – Москва, [2022]. - URL: https://urait.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. База данных «Электронная библиотека технического ВУЗа (ЭБС «Консультант студента») : электронно-библиотечная система : сайт / ООО Политехресурс. – Москва, [2022]. – URL: https://www.studentlibrary.ru/cgi-bin/mb4x. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Консультант врача. Электронная медицинская библиотека : база данных : сайт / ООО Высшая школа организации и управления здравоохранением-Комплексный медицинский консалтинг. – Москва, [2022]. – URL: https://www.rosmedlib.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО Букап. – Томск, [2022]. – URL: https://www.books-up.ru/ru/library/ . – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.6. ЭБС Лань : электронно-библиотечная система : сайт / ООО ЭБС Лань. – Санкт-Петербург, [2022]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. ЭБС **Znanium.com :** электронно-библиотечная система : сайт / ООО Знаниум. - Москва, [2022]. - URL: http://znanium.com . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

1.8. Clinical Collection : научно-информационная база данных EBSCO // 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. База данных «Русский как иностранный» : электронно-образовательный ресурс для иностранных студентов : сайт / ООО Компания «Ай Пи Ар Медиа». – Саратов, [2022]. – 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, [2022].

3. Базы данных периодических изданий:

3.1. База данных периодических изданий EastView : электронные журналы / ООО ИВИС. - Москва, [2022]. – 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, [2022]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

3.3. Электронная библиотека «Издательского дома «Гребенников» (Grebinnikon) : электронная библиотека / ООО ИД Гребенников. – Москва, [2022]. – URL:

https://id2.action-media.ru/Personal/Products. – Режим доступа : для авториз. пользователей. – Текст : электронный.

4. Федеральная государственная информационная система «Национальная электронная библиотека» : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2022]. – URL: https://нэб.рф. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. SMART Imagebase : научно-информационная база данных EBSCO // 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 . – URL: http://window.edu.ru/ . – Текст : электронный.

6.2. Российское образование : федеральный портал / учредитель ФГАУ «ФИЦТО». – URL: http://www.edu.ru. – Текст : электронный.

7. Образовательные ресурсы УлГУ:

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

Согласовано:

Заместитель начальника УИТиТ /Клочкова А.В. _____/ 04.05.2022

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Аудитория -3/316. Аудитория для проведения лекционных, семинарских и практических занятий, текущего контроля и промежуточной аттестации, групповых и индивидуальных консультаций. Комплект переносного мультимедийного оборудования: ноутбук с выходом в Интернет, экран, проектор, Wi-Fi с доступом в Интернет, ЭИОС,ЭБС. 432017, Ульяновская область, г. Ульяновск, ул. Набережная реки Свияги, д. 106-3 корпус

Помещение 503. Аудитория для проведения практических и лабораторных занятий, текущего контроля и промежуточной аттестации, групповых и индивидуальных консультаций. Помещение укомплектовано ученической доской и комплектом мебели (посадочных мест – 10). Компьютеры, Wi-Fi с доступом к сети «Интернет», ЭИОС, ЭБС. 432017, Ульяновская область, г. Ульяновск, р-н Железнодорожный, ул. Набережная р. Свияги, № 106 (1 корпус).

Аудитория 24б для проведения лабораторных и практических занятий, текущего контроля и промежуточной аттестации, групповых и индивидуальных консультаций. 11 персональных компьютеров, проектор, экран, системы защиты информации: Соболь, Аккорд, Dallas Lock, Secret Net Studio. Сервер Vimark, АПКШ "Континент", Маршрутизаторы Cisco, Система защиты информации ViPNet. 432017, Ульяновская обл, г Ульяновск, ул Набережная реки Свияги, д 106-2 корпус

Аудитория -230. Аудитория для самостоятельной работы. Аудитория укомплектована ученической мебелью. 16 персональных компьютеров. 432017, Ульяновская область, г. Ульяновск, р-н Железнодорожный, ул. Набережная р. Свияги, № 106-1 корпус

Аудитория -237. Читальный зал научной библиотеки с зоной для самостоятельной работы. Аудитория укомплектована ученической мебелью. Компьютерная техника, телевизор, экран, проектор. Стол для лиц с ОВЗ. 432017, Ульяновская область, г. Ульяновск, р-н Железнодорожный, ул. Набережная р. Свияги, № 106-1 корпус.

13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающимся) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических возможностей:

- для лиц с нарушением зрения: в форме электронного документа, индивидуальные консультации с привлечением тифлосурдопереводчика, индивидуальные задания и консультация;
- для лиц с нарушением слуха: в форме электронного документа, индивидуальные консультации с привлечением сурдопереводчика, индивидуальные задания и консультация;
- для лиц с нарушением опорно-двигательного аппарата: в форме электронного документа, индивидуальные задания и консультация.

В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий, организация работы ППС с обучающимися с ОВЗ и инвалидами предусматривается в электронной информационно-образовательной среде с учетом их индивидуальных психофизических особенностей.

Разработчик _____ / Ганеев С.М. /
подпись ФИО