

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	Криптографические протоколы
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 изучения дисциплины:

- изучение принципов построения и алгоритмов протоколов, обеспечивающих конфиденциальность, целостность и аутентичность информации.

Задачи изучения дисциплины:

- обучить студентов принципам работы основных протоколов;
- привить студентам навыки реализации криптографических протоколов с использованием ЭВМ;
- дать студентам представление об анализе стойкости протоколов к атакам.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к обязательной части цикла Б1 образовательной программы и читается в 10-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), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины «Криптографические протоколы» направлен на формирование следующих компетенций.

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
ОПК-8 – Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей	Знать: алгоритмы проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в конечных циклических группах; Уметь: проводить вычисления в числовых и конечных кольцах и полях с подстановками, многочленами, матрицами, в том числе с использованием компьютерных программ; Владеть: навыками эффективного вычисления в кольцах вычетов и в кольцах многочленов.
ОПК-10 – Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации	Знать: основные типы криптопротоколов и принципов их построения с использованием шифрсистем Уметь:

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

при решении задач профессиональной деятельности	проводить анализ криптографических протоколов, в том числе с использованием автоматизированных средств Владеть: подходами к разработке и анализу безопасности криптографических протоколов
---	--

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего) 4.

4.2. Объем дисциплины по видам учебной работы:

Вид учебной работы	Количество часов (форма обучения - дневная)			
	Всего по плану	В т.ч. по семестрам		
		10		
Контактная работа обучающихся с преподавателем	30/30*	30/30*		
Аудиторные занятия:				
• Лекции	30/30*	30/30*		
• Практические и семинарские занятия				
• Лабораторные работы (лабораторный практикум)	30/30*	30/30*		
Самостоятельная работа	48	48		
Экзамен	36	36		
Форма текущего контроля знаний и контроля самостоятельной работы		Лабораторные работы, проверка решения задач		
Всего часов по дисциплине	144	144		
Виды промежуточного контроля (экзамен, зачет)		экзамен		
Общая трудоемкость в зач. ед.	4	4		

**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*

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

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 интерактивной форме	Самостоятельная работа		
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы				
1	2	3	4	5	6	7		
Раздел 1. Протоколы аутентификации								
1. Протоколы аутентификации, использующие технику «запрос–ответ»	17	5					12	
2. Протоколы аутентификации с нулевым разглашением	37	10		15	6	12		Лабораторная работа. Домашние задания
Раздел 2. Протоколы передачи ключей								
3. Протоколы с нулевым разглашением	32	5		15	6	12		Лабораторная работа. Домашние задания
4. Протоколы передачи ключей	22	10				12		
Экзамен	36							
Итого:	144	30		30	12	48		

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Раздел 1. Протоколы аутентификации

Тема 1. Протоколы аутентификации, использующие технику «запрос–ответ»

Протоколы аутентификации, использующие пароли (слабая аутентификация). Протоколы аутентификации, использующие технику «запрос–ответ»: «запрос–ответ» с использованием симметричных алгоритмов шифрования. Протоколы аутентификации, использующие технику «запрос–ответ»: «запрос–ответ» с использованием асимметричных алгоритмов шифрования.

Тема 2. Протоколы аутентификации с нулевым разглашением

Протокол аутентификации Фиата-Шамира. Протокол Фейга-Фиата-Шамира. Итеративный протокол аутентификации Фиата-Шамира без доверенного центра. Трехпроходный протокол аутентификации Фиата-Шамира без доверенного центра. Протокол аутентификации Шнорра. Итеративный и трехпроходный модифицированный протокол Шнорра. Модификация протокола Шнорра на эллиптических кривых. Итеративный и трехпроходный модифицированный протокол Шнорра на эллиптических кривых. Протокол аутентификации Окамото. Модификация протокола Окамото на эллиптических кривых. Протокол аутентификации Гиллоу-Куискатр (GQ). Протокол аутентификации с нулевым разглашением на основе доказательства изоморфизма графов. Пятипроходный протокол аутенти-

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

фикации на основе изоморфизма графов с использованием эллиптических кривых. Протокол аутентификации с нулевым разглашением на основе асимметричных шифров. Протокола аутентификации с нулевым разглашением на основе шифра RSA. Протокола аутентификации с нулевым разглашением на основе шифра Эль-Гамала. Модификация протокола аутентификации с нулевым разглашением на основе шифра Эль-Гамала с использованием эллиптических кривых. Модификация протокола аутентификации с нулевым разглашением на основе системы Диффи-Хеллмана с использованием эллиптических кривых.

Раздел 2. Протоколы передачи ключей

Тема 3. Протоколы с нулевым разглашением

Протокол подбрасывания монеты по телефону. Протокол типа “подбрасывание монеты по телефону” с использованием эллиптических кривых. Протоколы привязки к биту. Протокол привязки к биту на основе протокола Шнорра с использованием эллиптических кривых.

Тема 4. Протоколы передачи ключей

Передача ключей с использованием симметричного шифрования: двусторонние протоколы. Передача ключей с использованием симметричного шифрования: трехсторонние протоколы. Протокол Kerberos. Передача ключей с использованием асимметричного шифрования. Открытое распределение ключей. Протоколы МТИ. Модификация семейства протоколов МТИ на эллиптических кривых. Предварительное распределение ключей. Схема Блома.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

Практические (семинарские) занятия не предусмотрены учебным планом.

7. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)

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.

Полные задания для лабораторных работ приводятся в учебно-методическом пособии: Рацеев С.М. Лабораторный практикум по криптографическим протоколам [Электронный ресурс] / С. М. Рацеев; УлГУ, ФМИАТ, Каф. информ. безопасности и теории управления. - Ульяновск : УлГУ, 2019.

Раздел 1. Протоколы аутентификации

Тема 2. Протоколы аутентификации с нулевым разглашением

Цель работы: освоить методику работы протоколов аутентификации.

Задание. Требуется реализовать протокол аутентификации Фиата-Шамира.

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

Раздел 2. Протоколы передачи ключей

Тема 3. Протоколы с нулевым разглашением

Цель работы: изучение протоколов привязки к биту.

Задание. Реализовать протокол привязки к биту на основе протокола Шнорра.

Методические указания: основное внимание должно быть уделено освоению протоколов привязки к биту.

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

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

Курсовые и контрольные работы не предусмотрены учебным планом дисциплины.

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ

Протоколы аутентификации

1. Протоколы аутентификации, использующие пароли (слабая аутентификация).
2. Протоколы аутентификации, использующие технику «запрос–ответ»: «запрос–ответ» с использованием симметричных алгоритмов шифрования.
3. Протоколы аутентификации, использующие технику «запрос–ответ»: «запрос–ответ» с использованием асимметричных алгоритмов шифрования.

Протоколы аутентификации с нулевым разглашением знания

4. Протокол аутентификации Фиата-Шамира.
5. Протокол Фейга-Фиата-Шамира.
6. Итеративный протокол аутентификации Фиата-Шамира без доверенного центра.
7. Трехпроходный протокол аутентификации Фиата-Шамира без доверенного центра.
8. Протокол аутентификации Шнорра.
9. Итеративный и трехпроходный модифицированный протокол Шнорра.
10. Модификация протокола Шнорра на эллиптических кривых.
11. Итеративный и трехпроходный модифицированный протокол Шнорра на эллиптических кривых.
12. Протокол аутентификации Окамото.
13. Модификация протокола Окамото на эллиптических кривых.
14. Протокол аутентификации Гиллоу-Куискатр (GQ).
15. Протокол аутентификации с нулевым разглашением на основе доказательства изоморфизма графов.
16. Пятипроходный протокол аутентификации на основе изоморфизма графов с использованием эллиптических кривых.
17. Протокол аутентификации с нулевым разглашением на основе асимметричных шифров.
18. Протокола аутентификации с нулевым разглашением на основе шифра RSA.
19. Протокола аутентификации с нулевым разглашением на основе шифра Эль-Гамала.
20. Модификация протокола аутентификации с нулевым разглашением на основе шифра Эль-Гамала с использованием эллиптических кривых.
21. Модификация протокола аутентификации с нулевым разглашением на основе системы Диффи-Хеллмана с использованием эллиптических кривых.

Протоколы с нулевым разглашением

22. Протокол подбрасывания монеты по телефону.
23. Протокол типа “подбрасывание монеты по телефону” с использованием эллиптических кривых.
24. Протоколы привязки к биту.
25. Протокол привязки к биту на основе протокола Шнорра с использованием эллиптических кривых.

Протоколы передачи ключей

26. Передача ключей с использованием симметричного шифрования: двусторонние протоколы.
27. Передача ключей с использованием симметричного шифрования: трехсторонние протоколы. Протокол Kerberos.

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

28. Передача ключей с использованием асимметричного шифрования.
29. Открытое распределение ключей. Протоколы МТИ.
30. Модификация семейства протоколов МТИ на эллиптических кривых.
31. Предварительное распределение ключей. Схема Блома.

10. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

Название разделов и тем	Вид самостоятельной работы	Объем в часах	Форма контроля
1. Протоколы аутентификации, использующие технику «запрос–ответ»	Проработка учебного материала, подготовка к зачету	12	Экзамен
2. Протоколы аутентификации с нулевым разглашением	Проработка учебного материала, лабораторные работы, подготовка к зачету, решение задач	12	Проверка лабораторных работ, экзамен, проверка решения задач
3. Протоколы с нулевым разглашением	Проработка учебного материала, лабораторные работы, подготовка к зачету	12	Проверка лабораторных работ, экзамен
4. Протоколы передачи ключей	Проработка учебного материала, подготовка к зачету	12	Экзамен

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. Запечников, С. В. Криптографические методы защиты информации : учебник для академического бакалавриата / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2019. — 309 с. — (Высшее образование). — ISBN 978-5-534-02574-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://biblionline.ru/bcode/433133>
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. Лабораторный практикум по криптографическим протоколам / С. М. Рацеев; УлГУ, ФМИАТ, Каф. информ. безопасности и теории управления. - Ульяновск : УлГУ, 2019. - URL: <http://lib.ulsu.ru/MegaPro/Download/MObject/1344>
3. Рацеев С. М. Методические указания для самостоятельной работы студентов по дисциплине «Криптографические протоколы» 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 : 128 КБ). - Текст : электронный. Режим доступа: <http://lib.ulsu.ru/MegaPro/Download/MObject/4686>

Согласовано:

П.А.Сиб-рь К.В. УлГУ Полкина И.Ю В.И. 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

