УТВЕРЖДЕНО

решением Ученого совета факультета математики,
информационных и авиационных технологий
от «21» 05 2024г., протокол №_5/24__
Председатель _____Волков М.А._
«_21_» ____05_ _____ 2024_ _____г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	**Криптографические протоколы**
Факультет	Факультет математики, информационных и авиационных технологий
Кафедра	Кафедра информационной безопасности и теории управления
Курс	5

Направление (специальность): 10.05.03 Информационная безопасность автоматизированных систем
Направленность (профиль/специализация): Безопасность открытых информационных систем
Форма обучения: очная
Дата введения в учебный процесс УлГУ: 01.09.2024 г.
Программа актуализирована на заседании кафедры: протокол №_10__ от _15.04_ 2024_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	Кафедра информационной безопасности и теории управления	Профессор,Доктор физико-математических наук, Доцент

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины:

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

Задачи освоения 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 «Криптографические протоколы» относится к числу дисциплин блока Б1.О.1, предназначенного для студентов, обучающихся по направлению: 10.05.03 Информационная безопасность автоматизированных систем.

В процессе изучения дисциплины формируются компетенции: ОПК-8, ОПК-10.

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: Криптографические протоколы, Теоретико-числовые методы в криптографии, Научно-исследовательская работа, Подготовка к сдаче и сдача государственного экзамена, Программно-аппаратные средства защиты информации, Основы информационной безопасности, Разработка и эксплуатация автоматизированных систем в защищенном исполнении, Организация электронно вычислительных машин и вычислительных систем.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

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 защиты информации в автоматизированных системах;	**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.

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
ОПК-10 Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности;	**знать**: основные типы криптопротоколов и принципов их построения с использованием шифрсистем **уметь**: 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): 3 ЗЕТ

4.2. Объем дисциплины по видам учебной работы (в часах): 108 часов

Форма обучения: очная

Вид учебной работы	Количество часов (форма обучения очная)	
	Всего по плану	В т.ч. по семестрам
		10
1	2	3
Контактная работа обучающихся с преподавателем в соответствии с УП	40	40
Аудиторные занятия:	40	40
Лекции	20	20
Семинары и практические занятия	-	-
Лабораторные работы, практикумы	20	20
Самостоятельная работа	68	68
Форма текущего контроля знаний и контроля самостоятельной работы: тестирование, контр. работа, коллоквиум, реферат и др. (не менее 2 видов)	Тестирование	Тестирование
Курсовая работа	-	-
Виды промежуточной аттестации (экзамен, зачет)	Зачет (0)	Зачет
Всего часов по дисциплине	108	108

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	8
Раздел 1. Протоколы аутентификации и передачи ключей							
Тема 1.1. Протоколы аутентификации.	28	4	0	10	0	14	Тестирование
Тема 1.2. Протоколы передачи ключей	28	4	0	10	0	14	Тестирование
Раздел 2. Безопасные многосторонние вычисления							
Тема 2.1. Протоколы для случая пассивного противника.	36	8	0	0	0	28	Тестирование
Тема 2.2. Протоколы для случая активного противника.	16	4	0	0	0	12	Тестирование
Итого подлежит изучению	108	20	0	20	0	68	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Протоколы аутентификации и передачи ключей

Тема 1.1. Протоколы аутентификации.

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. 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 аутентификации 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-Гамаля. Модификация протокола аутентификации с нулевым разглашением на основе шифра Эль-Гамаля с использованием эллиптических кривых. Модификация протокола аутентификации с нулевым разглашением на основе системы Диффи-Хеллмана с использованием эллиптических кривых.

Тема 1.2. 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 MTI. Модификация семейства протоколов MTI на эллиптических кривых. Предварительное распределение ключей. Схема Блома.

Раздел 2. Безопасные многосторонние вычисления

Тема 2.1. Протоколы для случая пассивного противника.

Вычислительная неразличимость. Семейства неравномерных схем. Вычислительная безопасность. IND-CPA безопасность. Одноразовые коды аутентификации. Случайный оракул. Схемы обязательств. Подбрасывание монеты. Псевдослучайные генераторы. Псевдослучайные функции. Широковещательная передача. Модели противника. Парадигма “реальный-идеальный”. Пассивный противник и честное большинство. Протокол BGW. t-конфиденциальность протокола BGW. Метод t-конфиденциального вычисления произведения GRR. Численный пример протокола BGW. Забывчивая передача. Забывчивая передача на основе асимметричных шифров. Протокол забывчивой передачи Белларе-Микали. Забывчивая передача на основе перестановок с лазейками. Забывчивая передача Наора-Пинкаса на основе проблемы DDH. Случайная забывчивая передача. Протокол IKNP расширения забывчивой передачи. Стандартное и корреляционное расширения забывчивой передачи. Забывчивая передача 1 из n Наора-Пинкаса. Забывчивая передача k из n на основе предположения DDH. Пассивный противник и нечестное большинство. Протокол GMW для логической схемы. Протокол GMW для логической схемы. Метод IPS для безопасного произведения. Протоколы на основе искаженных схем. Искаженные схемы Яо.

Тема 2.2. Протоколы для случая активного противника.

Проверяемые схемы разделения секрета. Протокол BGW. t-безопасность протокола BGW. Метод t-безопасного вычисления произведения на основе протокола AAPP. Активный противник и нечестное большинство. Конструкция BDOZ. Конструкция SPDZ. Протокол DGNNT на основе BDOZ и OLE.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

7. ЛАБОРАТОРНЫЕ РАБОТЫ, ПРАКТИКУМЫ

Протокол Фиата-Шамира.
Цели: Освоить методику работы протоколов аутентификации.
Содержание: Требуется реализовать протокол аутентификации Фиата-Шамира.
Результаты: Основное внимание должно быть уделено освоению протоколов аутентификации.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/270
Протокол Kerberos.
Цели: Освоить методику работы протоколов передачи ключей.
Содержание: Реализовать протокол Kerberos.
Результаты: Основное внимание должно быть уделено освоению протоколов передачи ключей.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/270

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

Данный вид работы не предусмотрен УП.

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ

1. Протоколы аутентификации, использующие технику «запрос–ответ»: «запрос–ответ» с использованием симметричных алгоритмов шифрования.

2. Протоколы аутентификации, использующие технику «запрос–ответ»: «запрос–ответ» с использованием асимметричных алгоритмов шифрования и электронной подписи.

3. Протокол аутентификации Фиата-Шамира.

4. Протокол Фейга-Фиата-Шамира.

5. Протокол аутентификации Шнорра.

6. Протокол аутентификации Окамото.

7. Протокол аутентификации Гиллоу-Куискатр (GQ).

8. Протокол аутентификации с нулевым разглашением на основе доказательства изоморфизма графов.

9. Протокол аутентификации с нулевым разглашением на основе асимметричных шифров.

10. Передача ключей с использованием симметричного шифрования: двусторонние протоколы.

11. Передача ключей с использованием симметричного шифрования: трехсторонние протоколы. Протокол Kerberos.

12. Передача ключей с использованием асимметричного шифрования.

13. Схемы разделения секрета на основе линейных кодов.

14. Синхронные проверяемые схемы разделения секрета.

15. Методы GRR вычисления произведения.

16. Протокол BGW для случая пассивного противника.

17. Проверяемая синхронная схема разделения секрета.

18. Забывчивая передача.

19. Протокол GMW для логической схемы.

20. Протокол Яо.

21. Протокол AFLNO.

22. Протокол BGW для две трети честного большинства.

23. Конструкция BDOZ.

24. Конструкция SPDZ.

25. Протоколы с прерыванием, активным противником и

26. честным большинством.

10. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩИХСЯ

Содержание, требования, условия и порядок организации самостоятельной работы обучающихся с учетом формы обучения определяются в соответствии с «Положением об организации самостоятельной работы обучающихся», утвержденным Ученым советом УлГУ (протокол №8/268 от 26.03.2019г.).

По каждой форме обучения: очная/заочная/очно-заочная заполняется отдельная таблица

Форма обучения: очная

Название разделов и тем	**Вид самостоятельной работы** ***(проработка учебного материала, решение задач, реферат, доклад, контрольная работа,подготовка к сдаче зачета, экзамена и др).***	**Объем в часах**	**Форма контроля** ***(проверка решения задач, реферата и др.)***
Раздел 1. Протоколы аутентификации и передачи ключей			
Тема 1.1. Протоколы аутентификации.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	14	Тестирование
Тема 1.2. Протоколы передачи ключей	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	14	Тестирование
Раздел 2. Безопасные многосторонние вычисления			
Тема 2.1. Протоколы для случая пассивного противника.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	28	Тестирование
Тема 2.2. Протоколы для случая активного противника.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	12	Тестирование

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы

основная

1. Рацеев Сергей Михайлович. Математические методы защиты информации : учебное пособие для вузов / С.М. Рацеев. - Санкт-Петербург : Лань, 2023. - 543 с. - (Высшее образование). - ISBN 978-5-8114-8589-5 (в пер.). / .— ISBN 1_258181

2. Черемушкин Александр Васильевич. Криптографические протоколы. Основные свойства и уязвимости : учеб. пособие для вузов по спец. "Компьютер. безопасность" / А.В. Черемушкин. - Москва : Академия, 2009. - 272 с. : ил. - (Высшее профессиональное образование) (Информационная безопасность). - Библиогр.: с. 264-270. - ISBN 978-5-7695-5748-4 (в пер.). / .— ISBN 1_182853

дополнительная

1. Рацеев Сергей Михайлович. Математические методы защиты информации и их основы. Сборник

задач : учебное пособие для вузов / С.М. Рацеев. - Санкт-Петербург : Лань, 2023. - 136 с. - (Высшее образование). - Библиогр.: с. 135-136. - ISBN 978-5-507-45197-5 (в пер.). / .— ISBN 1_258183

2. Косолапов, Ю. В. Криптографические протоколы на основе линейных кодов : учебное пособие / Ю. В. Косолапов ; Ю. В. Косолапов. - Ростов-на-Дону, Таганрог : Издательство Южного федерального университета, 2020. - 98 с. - Книга находится в премиум-версии ЭБС IPR BOOKS. - Текст. - Весь срок охраны авторского права. - электронный. - Электрон. дан. (1 файл). - URL: http://www.iprbookshop.ru/100176.html. - Режим доступа: ЭБС IPR BOOKS; для авторизир. пользователей. - ISBN 978-5-9275-3316-9. / .— ISBN 0_156357

учебно-методическая

1. Рацеев С. М. Методические указания для самостоятельной работы студентов по дисциплине «Криптографические протоколы» для студентов специальностей 10.05.01 «Компьютерная безопасность» и 10.05.03 «Информационная безопасность автоматизированных систем» / С. М. Рацеев. - 2022. - 6 с. - Неопубликованный ресурс. - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/13335. - Режим доступа: ЭБС УлГУ. - Текст : электронный. / .— ISBN 0_475960.

б) Программное обеспечение

- Операционная система "Альт образование"
- Офисный пакет "Мой офис"
- Visual studio code

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, [2024]. – 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, [2024]. - 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, [2024]. – 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, [2024]. – URL: https://www.rosmedlib.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО Букап. –

Томск, [2024]. – 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, [2024]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. ЭБС **Znanium.com** : электронно-библиотечная система : сайт / ООО Знаниум. - Москва, [2024]. - URL: http://znanium.com . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. /ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2024].

3. eLIBRARY.RU: научная электронная библиотека : сайт / ООО «Научная Электронная Библиотека». – Москва, [2024]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

4. Федеральная государственная информационная система «Национальная электронная библиотека» : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2024]. – URL: https://нэб.рф. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

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

6. 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.

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

Аудитории для проведения лекций, семинарских занятий, для выполнения лабораторных работ и практикумов, для проведения текущего контроля и промежуточной аттестации, курсового проектирования, групповых и индивидуальных консультаций *(выбрать необходимое)*

Аудитории укомплектованы специализированной мебелью, учебной доской. Аудитории для проведения лекций оборудованы мультимедийным оборудованием для представления информации большой аудитории. Помещения для самостоятельной работы оснащены компьютерный техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде, электронно-библиотечной системе. Перечень оборудования, используемого в учебном процессе:

- Мультимедийное оборудование: компьютер/ноутбук, экран, проектор/телевизор
- Компьютерная техника

13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

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

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации;
- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации;
- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

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	Доктор физико-математических наук, Доцент	Рацеев Сергей Михайлович
	Должность, ученая степень, звание	ФИО