Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

Кафедра алгебры и дискретной математики

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б.1.В.ДВ.5.1 Криптографические протоколы»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки
02.03.01 Математика и компьютерные науки
(код и наименование направления подготовки)

Алгоритмы и приложения компьютерной математики
(наименование направленности (профиля) образовательной программы)

Тип образовательной программы
Программа академического бакалавриата

Квалификация
Бакалавр

Форма обучения
Очная

Год набора 2017

Рабочая программа рассмотрена и утверждена на заседании кафедры

Кафедра алгебры и дискретной математики
наименование кафедры

протокол 7 от "21" февраля 2017 г.

Заведующий кафедрой
Кафедра алгебры и дискретной математики _____ О.А. Пихтилькова
наименование кафедры *подпись* *расшифровка подписи*

Исполнители:
старший преподаватель _____ А.Н. Благовисная
должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по направлению подготовки
02.03.01 Математика и компьютерные науки _____ О.А. Пихтилькова
код наименование *личная подпись* *расшифровка подписи*

Заведующий отделом комплектования научной библиотеки
_____ Н.Н. Грицай
личная подпись *расшифровка подписи*

Уполномоченный по качеству факультета
_____ И.В. Крючкова
личная подпись *расшифровка подписи*

№ регистрации _____

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:

формирование системы знаний о правилах, регламентирующих использование криптографических преобразований и алгоритмов в информационных процессах, развитие навыков решения задач, связанных с преобразованием и передачей информации.

Задачи:

- *изучение базовых криптографических протоколов, используемых при исследовании и построении современных алгоритмов, методов и моделей преобразования и защиты информации;*
- *овладение основными методами анализа и реализации криптографических протоколов;*
- *приобретение навыков решения теоретических и практических задач защищенной передачи информации.*

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к дисциплинам (модулям) по выбору вариативной части блока 1 «Дисциплины (модули)»

Пререквизиты дисциплины: *Б.1.Б.13 Математический анализ, Б.1.Б.14 Фундаментальная и компьютерная алгебра, Б.1.Б.16 Дискретная математика, математическая логика и их приложения в информатике и компьютерных науках*

Постреквизиты дисциплины: *Отсутствуют*

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
Знать: - *математические основы построения правил, регламентирующих использование криптографических преобразований и алгоритмов в информационных процессах;* **Уметь:** - *решать задачи алгебры, математической логики, теории чисел, дискретной математики, возникающие при построении различных криптографических протоколов;* **Владеть:** - *навыками интерпретации математических моделей процессов передачи и преобразования информации.*	ОПК-1 готовностью использовать фундаментальные знания в области математического анализа, комплексного и функционального анализа, алгебры, аналитической геометрии, дифференциальной геометрии и топологии, дифференциальных уравнений, дискретной математики и математической логики, теории вероятностей, математической статистики и случайных процессов, численных методов, теоретической механики в будущей профессиональной деятельности
Знать: - *криптографические стандарты;* - *типовые криптографические протоколы и основные требования к*	ПК-1 способностью к определению общих форм и закономерностей отдельной

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
ним; *- основные схемы цифровой подписи;* *- протоколы идентификации;* *- протоколы передачи и распределения ключей;* **Уметь:** *- использовать симметричные и асимметричные криптоалгоритмы для построения криптографических протоколов;* *- проводить сравнительный анализ криптографических протоколов, решающих сходные задачи;* **Владеть:** *- криптографической терминологией.*	предметной области
Знать: *- формулировки и доказательства всех утверждений курса;* **Уметь:** *- формулировать задачу по оцениванию безопасности криптографического протокола применительно к конкретным условиям;* *- формулировать свойства безопасности криптографических протоколов;* **Владеть:** *- простейшими методами анализа безопасности криптографических протоколов.*	ПК-3 способностью строго доказать утверждение, сформулировать результат, увидеть следствия полученного результата

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единиц (144 академических часов).

Вид работы	Трудоемкость, академических часов	
	7 семестр	всего
Общая трудоёмкость	**144**	**144**
Контактная работа:	**35,25**	**35,25**
Лекции (Л)	18	18
Лабораторные работы (ЛР)	16	16
Консультации	1	1
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;* *- подготовка к лабораторным занятиям;* *- подготовка к устным и письменным опросам;* *- подготовка к рубежному контролю)*	**108,75**	**108,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**экзамен**	

Разделы дисциплины, изучаемые в 7 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Общие сведения о криптографических протоколах	46	6		0	20
2	Протоколы идентификации и аутентификации	34	8		8	44
3	Протоколы распределения ключей	38	8		8	46
	Итого:	144	18		16	110
	Всего:	144	18		16	110

4.2 Содержание разделов дисциплины

№ 1 Общие сведения о криптографических протоколах

Понятие протокола и его основные характеристики. Понятие криптографического протокола. Виды криптографических протоколов. Свойства безопасных криптографических протоколов.

№ 2 Протоколы идентификации и аутентификации

Понятия идентификации и аутентификации. Слабая и сильная аутентификация. Слабая аутентификация на основе фиксированных паролей. Атаки на фиксированные пароли. Правила составления паролей. Методы хранения паролей в системах. Схемы использования паролей. Сильная аутентификация типа «запрос-ответ». «Запрос-ответ» на основе симметричных и асимметричных алгоритмов шифрования. Протоколы аутентификации, использующие цифровую подпись. Протоколы идентификации, использующие технику доказательства знания.

№ 3 Протоколы распределения ключей

Типы протоколов распределения ключей: протоколы обмена ключей, протоколы открытого распределения ключей и схемы предварительного распределения ключей.

Протоколы передачи ключей с использованием симметричного шифрования. Двусторонние протоколы передачи ключей с использованием симметричного шифрования. Протоколы типа «запрос-ответ» и его модификации. Использование односторонней функции. «Бесключевой» протокол Шамира и его модификации. Трехсторонние протоколы: виды и атаки. Протоколы широкоротой лягушки, Yahalom, Нидхейма-Шредера, Отвей-Риса, Kerberos и их модификации.

Использование асимметричного шифрования для передачи ключей симметричных криптосистем. Протоколы без использования цифровой подписи: одношаговый протокол, протокол NSPK, протокол Woo-Lam. Смешанные протоколы. Использование цифровой подписи. Сертификаты открытых ключей.

Открытое распределение ключей и его отличие от распределения открытых ключей. Понятие безопасного аутентификационного протокола обмена ключами. Протокол Диффи-Хеллмана, его достоинства и недостатки. Атака «человек посередине» и методы защиты от неё. Аутентифицированные протоколы.

Предварительное распределение ключей. Проблема предварительного распределения ключей. Свойства схем предварительного распределения ключей. Примеры схем предварительного распределения ключей между n абонентами. Схемы разделения секрета.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	2	Протоколы идентификации, использующие пароли.	2
2	2	Протоколы сильной аутентификации.	2
3	2	Протоколы идентификации, использующие технику доказательства знания.	2
4	3	Протоколы передачи ключей с использованием симметричного шифрования.	4
5	3	Протоколы передачи ключей с использованием асимметричного шифрования.	4
6	3	Схемы предварительного распределения ключей.	2
		Итого:	16

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Ищукова, Е.А. Криптографические протоколы и стандарты: учебное пособие [Электронный ресурс] / Е.А. Ищукова, Е.А. Лобова; Министерство образования и науки РФ, Южный федеральный университет, Инженерно-технологическая академия. – Таганрог: Издательство Южного федерального университета, 2016. – 80 с. – Режим дотупа: http://biblioclub.ru/index.php?page=book&id=493059

2. Смарт, Н. Криптография [Текст] / Н. Смарт; пер. с англ. С. А. Кулешова; под ред. С. К. Ландо. – Москва: Техносфера, 2006. – 528 с.

3. Фомичев, В. М. Дискретная математика и криптология [Текст]: курс лекций / В. М. Фомичев. – М.: Диалог- МИФИ, 2003. – 400 с.

4. Шаньгин, В.Ф. Информационная безопасность и защита информации [Электронный ресурс] / В.Ф. Шаньгин. – Москва: ДМК Пресс, 2014. – 702 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=260320

5.2 Дополнительная литература

1. Судоплатов, С. В. Элементы дискретной математики [Текст] : учеб. для вузов / С. В. Судоплатов, Е. В. Овчинникова. – М.: ИНФРА-М ; Новосибирск : НГТУ, 2002. – 280 с.

2. Отрыванкина, Т.М. Алгоритмы компьютерной алгебры: практикум / Т. М. Отрыванкина; М-во образования и науки Рос. Федерации, Федер. агентство по образованию, Гос. образоват. учреждение высш. проф. образования «Оренбург. гос. ун-т», каф. приклад. математики. – Оренбург: ОГУ, 2007. – 26 с.

3. Введение в криптографию [Текст]: учебник / под ред. В. В. Ященко. – СПб.: Питер, 2001. – 288 с.

5.3 Периодические издания

1. Прикладная математика и механика: журнал. – М.: Агентство «Роспечать», 2016.

2. Вычислительные технологии: журнал. – М.: Агентство «Роспечать», 2016.

3. Вестник компьютерных и информационных технологий: журнал. – М.: Агентство «Роспечать», 2017.

4. Информационные технологии: журнал. – М.: Агентство «Роспечать», 2017.

5.4 Интернет-ресурсы

1. http://cryptography.ru – сайт посвящен вопросам математической криптографии, содержит календарь конференций, семинаров и т. п., которые полностью или частично посвящены вопросам защиты информации, а также актуальные ссылки на сайты данных научных мероприятий.
2. http://eqworld.ipmnet.ru/indexr.htm – международный научно-образовательный сайт «Мир математических уравнений», который содержит обширную учебную физико-математическую библиотеку и предназначен для широкого круга ученых, преподавателей вузов, инженеров, аспирантов и студентов в различных областях математики и других наук; все ресурсы сайта являются бесплатными для его пользователей).
3. https://arxiv.org/ – крупнейший бесплатный архив электронных публикаций научных статей и их препринтов по физике, математике, астрономии, информатике и биологии.
4. «Криптографические протоколы» [Электронный ресурс]: онлайн-курс на платформе https://www.lektorium.tv/mooc – «Лекториум» / Разработчик курса: Computer Science клуб при ПОМИ РАН, режим доступа: https://www.lektorium.tv/course/22759

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы современных информационных технологий

1. Операционная система Microsoft Windows.
2. OpenOffice/LibreOffice - свободный офисный пакет программ, включающий в себя текстовый и табличный редакторы, редактор презентаций и другие офисные приложения.
3. Бесплатное средство просмотра файлов PDF Adobe Reader.
4. Microsoft Visual Studio (лицензии по программе Microsoft Dream Spark Premium).
5. SCOPUS [Электронный ресурс]: реферативная база данных / компания Elsevier. – Режим доступа: https://www.scopus.com/, в локальной сети ОГУ.
6. Springer [Электронный ресурс]: база данных научных книг, журналов, справочных материалов / компания Springer Customer Service Center GmbH. – Режим доступа: https://link.springer.com/, в локальной сети ОГУ.
7. Общероссийский математический портал Math-Net.Ru [Электронный ресурс]: профессиональная база данных для математиков – Режим доступа: http://www.mathnet.ru/index.phtml/?option_lang=rus

6 Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий семинарского типа, для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Аудитории оснащены комплектами ученической мебели, техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Для проведения лабораторных занятий используется лаборатория компьютерный класс, оснащенный компьютерной техникой.

Помещение для самостоятельной работы обучающихся оснащены компьютерной техникой подключенной к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду ОГУ.

К рабочей программе прилагаются:

- Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине;
- Методические указания для обучающихся по освоению дисциплины.