Минобрнауки России

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

Кафедра компьютерной безопасности и математического обеспечения информационных систем

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«С.1.Б.39 Криптографические протоколы»

Уровень высшего образования

СПЕЦИАЛИТЕТ

Специальность
10.05.01 Компьютерная безопасность
(код и наименование специальности)

Разработка защищенного программного обеспечения
(наименование направленности (профиля)/специализации образовательной программы)

Квалификация
Специалист по защите информации

Форма обучения
Очная

Год набора 2018

Рабочая программа рассмотрена и утверждена на заседании кафедры

Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры

протокол № 3 от "14" декабря 2017 г.

Заведующий кафедрой
Кафедра компьютерной безопасности и математического обеспечения информационных систем — И.В. Влацкая
наименование кафедры *подпись* *расшифровка подписи*

Исполнители:
доцент — Е.И. Ряполова
должность *подпись* *расшифровка подписи*

должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по специальности
10.05.01 Компьютерная безопасность — И.В. Влацкая
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 75225

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины: является изучение принципов построения и алгоритмов реализации протоколов, обеспечивающих конфиденциальность, целостность и аутентичность информации.

Задачи:

- освоение фундаментальных математических понятий криптологии;
- освоение базовых понятий, идей и алгоритмов, связанных с протоколами, применяемыми в криптографии;
- приобретение навыков реализации криптографических протоколов с использованием ЭВМ;
- формирование представлений об атаках на протоколы и методах противодействия.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к базовой части блока 1 «Дисциплины (модули)»

Пререквизиты дисциплины: *С.1.Б.38 Криптографические методы защиты информации*

Постреквизиты дисциплины: *С.1.В.ОД.4 Технология построения защищенных автоматизированных систем*

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: -основные математические и физические методы решения **Уметь:** - применять математический аппарат при решении профессиональных задач направленных на разработку криптографических средств защиты **Владеть:** -методами и средства разработки криптографических средств защиты	ОПК-1 способностью анализировать физические явления и процессы при решении профессиональных задач
Знать: - основные сведения из теории графов; - алгебру многочленов; - основные сведения из теории вероятности и математической статистики. **Уметь:** - применять указанные выше математические знания при решении учебных задач. **Владеть:** -навыками применения элементов математической логики и дискретной математики при решении задач	ОПК-2 способностью корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятности, математической статистики, теории информации, теоретико-числовых методов
Знать: - современную историю криптографии; - действующие стандарты шифрования данных; - современные асимметричные криптосистемы; - методы использования асимметричных шифров для решения про-	ПК-1 способностью осуществлять подбор, изучение и обобщение научно-технической информации, методических

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
блемы распределения ключей, для создания электронной цифровой подписи и соответствующие стандарты **Уметь:** - работать с научной литературой, нормативными документами **Владеть:** - навыками анализа и обобщения передового опыта в сфере профессиональной деятельности	материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов сфере профессиональной деятельности
Знать: - различия между абсолютной и вычислительной стойкостью; - принципы построения поточных и блочных симметричных шифров; - протоколы распределения симметричных ключей. **Уметь:** - реализовывать программно изученные алгоритмы шифрования и создания ЭЦП **Владеть:** навыками решения прикладных криптографических задач	ПК-2 способностью участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований
Знать: - современные стандарты шифрования **Уметь:** - анализировать выбранные средства защиты данных на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности **Владеть:** - способами и методами определения компьютерных систем на соответствие стандартам	ПК-3 способностью проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности
Знать: - основные математические методы защиты информации **Уметь:** - реализовывать алгоритмы защиты данных на основе математических методов **Владеть:** - навыками построения математических моделей элементов безопасности и разработки криптографических алгоритмов	ПК-4 способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единиц (180 академических часов).

Вид работы	Трудоемкость, академических часов	
	8 семестр	всего
Общая трудоёмкость	**180**	**180**
Контактная работа:	**76,25**	**76,25**
Лекции (Л)	46	46
Лабораторные работы (ЛР)	30	30
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;*	**103,75**	**103,75**

Вид работы	Трудоемкость, академических часов	
	8 семестр	всего
- подготовка к рубежному контролю; *- подготовка к зачету.*		
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**зачет**	

Разделы дисциплины, изучаемые в 8 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Введение в предмет	6	2	0	0	4
2	Протоколы подбрасывания монеты. Протоколы привязки к биту.	18	4	0	4	10
3	Разделение секрета. Пороговые схемы, разделение секрета для произвольной структуры доступа.	16	4	0	2	10
4	Системы доказательства с нулевым разглашением.	14	4	0	0	10
5	Аутентификация и идентификация. Парольные схемы разграничения доступа. Запрос-ответные схемы. Протоколы «рукопожатия».	18	4	0	4	10
6	Протоколы идентификации и аутентификации на основе схем с нулевым разглашением.	18	4	0	4	10
7	Протоколы установления подлинности. Схемы цифровой подписи.	16	4	0	2	10
8	Скрытый канал. Слепая подпись. Затемненная подпись.	18	4	0	4	10
9	Электронная монета.	16	4	0	2	10
10	Протокол игры в покер «по телефону»	14	4	0	2	8
11	Управление ключами. Протоколы выработки и распределения секретного ключа.	26	8	0	6	12
	Всего:	180	46	0	30	104

4.2 Содержание разделов дисциплины

Раздел №1. Введение в предмет
Криптографические протоколы и основные требования к ним. Классификация протоколов. Примитивные и прикладные протоколы. Требования полноты и корректности.

Раздел №2. Протоколы подбрасывания монеты. Протоколы привязки к биту
Протоколы подбрасывания монеты (электронная жеребьевка).Привязка к биту, различные протоколы привязки к биту.
Разделение секрета.

Раздел №3. Разделение секрета. Пороговые схемы, разделение секрета для произвольной структуры доступа
Группа доступа. Структура доступа. Протоколы разделения секретов.
Проверяемое разделение секрета.Протоколы конфиденциальных вычислений.

Раздел №4. Интерактивные системы доказательства
Доказательства для языков квадратичных невычетов, для неизоморфизма графов. Системы доказательства с нулевым разглашением. Полнота, корректность, нулевое разглашение. Доказательство изоморфизма графов.

Раздел №5. Аутентификация и идентификация Протоколы идентификации и аутентификации. Парольные схемы разграничения доступа. Запрос-ответные схемы. Протоколы «рукопожатия».

Раздел №6. Протоколы идентификации и аутентификации на основе схем с нулевым разглашением
Схема Фиата-Шамира, схема Файге-Фиата-Шамира, схема Шнорра, схема Брикеллла и МакКарли, протокол Окамото. Доказательство полноты и корректности для этих схем. Вопрос о нулевом разглашении.

Раздел №7. Протоколы установления подлинности. Схемы цифровой подписи
Подпись RSA, Рабина, Фиата-Шамира, Онга-Шнорра-Шамира. Эль-Гамаля, DSS. Неотрицаемая подпись Шаума-ван Антверпена.

Раздел №8. Скрытый канал. Слепая подпись. Затемненная подпись
Совершенно слепая подпись. Затемненная подпись. Применение слепых подписей.
Подписи со скрытым каналом. Скрытый канал на основе подписи Онга-Шнорра-Шамира. Подход к построению скрытого канала. Подписи, свободные от скрытого канала.

Раздел №9. Электронная монета
Банковские криптографические протоколы. Электронные деньги. Требования к схемам электронных денег. Применение слепой подписи в схемах электронных денег.

Раздел № 10. Протокол игры в покер «по телефону»
Требования к протоколу «Покер по телефону». Протоколы «игры в покер». Протокол честной раздачи карт. Применение протокола «Покер по телефону».

Раздел №11. Управление ключами. Протоколы выработки и распределения секретного ключа
Протоколы генерации ключей. Протоколы распределения ключей. Бесключевой протокол Шамира. Протокол Диффи-Хэллмана. Протокол Нидхейма-Шредера. Протокол Kerberos. Инфраструктура открытых ключей. PKI. Рекомендации X.509

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	2	Компьютерная реализация схем электронной жеребьевки и привязки к биту	4
2	3	Реализация пороговых схем разделения секрета и СРС для произвольной структуры доступа	2
3	5	Парольные схемы идентификации и схемы рукопожатия	4
4	6	Имитационное моделирование протоколов идентификации на основе ИСД с нулевым разглашением.	4
5	7	Стандарты цифровой подписи	2
6	8	Компьютерная реализация схем слепой подписи и скрытого канала	4
7	9	Имитационное моделирование схемы электронных денег с монетами одинакового достоинства	2
8	10	Компьютерная реализация протокола «Покер по телефону» для 3-х игроков	2
9	11	Компьютерная реализация схемы электронного голосования для 5-ти участников	2
10	11	Компьютерная реализация протокола передачи секретного ключа (работа в группах).	4
		Итого	30

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Смарт, Н. Криптография. – М.: Техносфера, 2006. – 528 с.
2. Спицын, В. Г. Информационная безопасность вычислительной техники [Электронный ресурс] / В. Г. Спицын – Электрон.текстовые дан. – Томск : Эль Контент, 2011. – Режим доступа: http://www.biblioclub.ru/book/208694/
3. Гультяева, Т.А.Основы теории информации и криптографии: конспект лекций [Электронный ресурс] / Т.А. Гультяева; Министерство образования и науки РФ, Новосибирский государственный технический университет. – Новосибирск: НГТУ, 2010. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=228963

5.2 Дополнительная литература

1. Полянская О.Ю. Горбатов В.С. Инфраструктуры открытых ключей: учеб. Пособие [Электронный ресурс] М.: Интернет-Университет Информационных Технологий, 2007. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=233206
2. Васильков А.В. Безопасность и управление доступом в информационных системах: Учебное пособие / А.В. Васильков, И.А. Васильков. - М.: Форум: НИЦ ИНФРА-М, 2013. - 368 с.: ил.; 60x90 1/16. - (Профессиональное образование). (переплет) ISBN 978-5-91134-360-6, 500 экз. – Режим доступа: http://znanium.com/bookread2.php?book=405313

5.3 Периодические издания

1 Информатика и системы управления: журнал. - М. : Агентство "Роспечать", 2019
2 Вестник компьютерных и информационных технологий: журнал. - М. : Агентство "Роспечать", 2019
3 Информационные технологии: журнал. - М. : Агентство "Роспечать", 2019

5.4 Интернет-ресурсы

https://www.coursera.org/learn/metody-i-sredstva-zashity-informacii – «Coursera», МООК: Методы и средства защиты информации

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

1. Операционная система Microsoft Windows
2. Open Office/LibreOffice – свободный офисный пакет программ, включающий в себя текстовый и табличный редакторы, редактор презентаций и другие офисные приложения.
3. MicrosoftVisualStudio – среда разработки приложений.

6 Материально-техническое обеспечение дисциплины

Занятия по дисциплине проводятся в аудиториях, оснащенных компьютерными и мультимедийными средствами. Рабочие станции студентов и преподавателя объединены в локальную компьютерную сеть с возможностью выхода в Интернет.

Лекционные занятия проводятся в аудиториях, оснащенных мультимедийным оборудованием.

Лабораторные занятия проходят в компьютерных классах, в которых установлено оборудование:

- системные блоки модели Intel Celeron;

- системные блоки модели Intel Pentium Core 2 Duo;
- мониторы модели Samsung 793 DF.