Минобрнауки России

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

Кафедра компьютерной безопасности и математического обеспечения информационных систем

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.Б.39 Криптографические протоколы»

Уровень высшего образования

СПЕЦИАЛИТЕТ

Специальность
10.05.01 Компьютерная безопасность
(код и наименование специальности)

специализация №3 «Разработка защищенного программного обеспечения»
(наименование направленности (профиля)/специализации образовательной программы)

Квалификация
Специалист по защите информации

Форма обучения
Очная

Год набора 2023

Рабочая программа дисциплины «*Б1.Д.Б.39 Криптографические протоколы*» рассмотрена и утверждена на заседании кафедры

Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры

протокол № 7 от "9" марта 2023 г.

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

Исполнители:
Доцент *должность* *подпись* Е.И. Ряполова *расшифровка подписи*

должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по специальности
10.05.01 Компьютерная безопасность *код наименование* *личная подпись* И.В. Влацкая *расшифровка подписи*

Заведующий отделом формирования фонда и научной обработки документов
личная подпись Н.Н. Бигалиева *расшифровка подписи*

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

№ регистрации 152596

© Ряполова Е.И., 2023
© ОГУ, 2023

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 Д «Дисциплины (модули)»

Пререквизиты дисциплины: *Б1.Д.Б.38 Методы и средства криптографической защиты информации*

Постреквизиты дисциплины: *Б1.Д.В.2 Технология построения защищенных автоматизированных систем*

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
ОПК-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10-В-3 Знает основные типы криптопротоколов и принципов их построения с использованием шифрсистем ОПК-10-В-4 Умеет проводить анализ криптографических протоколов, в том числе с использованием автоматизированных средств ОПК-10-В-5 Владеет подходами к разработке и анализу безопасности криптографических протоколов	**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 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:	**90,25**	**90,25**
Лекции (Л)	46	46
Лабораторные работы (ЛР)	44	44
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;*	**89,75**	**89,75**
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.	18	4	0	4	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	4	8
8	Скрытый канал. Слепая подпись. Затемненная подпись.	18	4	0	6	8
9	Электронная монета.	18	4	0	6	8
10	Протокол игры в покер «по телефону»	18	4	0	6	8
11	Управление ключами. Протоколы выработки и распределения секретного ключа.	22	8	0	6	8
	Итого:	180	46		44	90
	Всего:	180	46		44	90

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	4
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	4
6	8	Компьютерная реализация схем слепой подписи и скрытого канала	4
7	9	Имитационное моделирование схемы электронных денег с монетами одинакового достоинства	6
8	10	Компьютерная реализация протокола «Покер по телефону» для 3-х игроков	6
9	11	Компьютерная реализация схемы электронного голосования для 5-ти участников	6
10	11	Компьютерная реализация протокола передачи секретного ключа (работа в группах).	6
		Итого:	44

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Смарт, Н. Криптография. – М.: Техносфера, 2006. – 528 с.
2. Вычислительно сложные задачи теории чисел [Текст] : учебное пособие / Е. А. Гречников [и др.]; Мос. гос. ун-т им. М. В. Ломоносова. - Москва : Изд-во Моск. ун-та, 2012.

5.2 Дополнительная литература

1. Бабаш, А. В. Криптография. – М.: Солон-Пресс, 2007. – 512 с.
2. Виноградов И.М. Основы теории чисел [Текст] : учебник для вузов / И.М. Виноградов.- СПб.: Лань, 2009. - 176 с.

5.3 Периодические издания

1 Информатика и системы управления: журнал. - М. : Агентство "Роспечать", 2023
2 Вестник компьютерных и информационных технологий: журнал. - М. : Агентство "Роспечать", 2023
3 Информационные технологии: журнал. - М. : Агентство "Роспечать", 2023

5.4 Интернет-ресурсы

1. www.citforum.ru/ - портал аналитических и научных статей в области информационных технологий;

2. www.rsdn.ru - сайт Российской сети разработчиков ПО, содержит статьи по современным средствам программирования;

3. «Меры и средства защиты информации от несанкционированного доступа» [Электронный ресурс]: онлайн-курс на платформе https://openedu.ru/ - «Открытое образование»/ Разработчик курса: Университет ИТМО, режим доступа: https://openedu.ru/course/mipt/ISMMAUA/?session=urfu_spring_2023

4. «Защита информации» [Электронный ресурс]: онлайн-курс на платформе https://openedu.ru/ - «Открытое образование»/ Разработчик курса: Университет ИТМО, режим доступа: https://openedu.ru/course/hse/DATPRO/?session=2022

5. «Специализация IT Fundamentals for Cybersecurity » [Электронный ресурс]: онлайн-курс на платформе https://www.coursera.org / Разработчик курса: The Hong Kong University of science and technology режим доступа: https://www.coursera.org/specializations/it-fundamentals-cybersecurity

6. Криптографические протоколы [Электронный ресурс] : электронный курс в системе Moodle / Е.И. Ряполова, Оренб. гос. ун-т. – Электрон. дан. – Оренбург: ОГУ, [2022-2023].– Режим доступа: Электронные курсы ОГУ в системе обучения moodle. – https://moodle.osu.ru/course/view.php?id=2196

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. Интегрированная система решения математических, инженерно-технических и научных задач PTC MathCAD 14.0
4. Система автоматизированного проектирования Autocad: Электронные лицензии для образовательных целей доступны бесплатно после регистрации аккаунта преподавателя/студента. Режим доступа: https://www.autodesk.com/education/free-software/featured
5. Среда разработки программного обеспечения на языке Object Pascal для компилятора Free Pascal: Lazarus.

Доступна бесплатно. Разработчики: Cliff Baeseman, Shane Miller, Michael A. Hess и др. Режим доступа: http://www.lazarus-ide.org/

6. Интегрированная среда разработки на Javas IntelliJ IDEA Community. Доступна бесплатно после регистрации преподавателя. Разработчик: компания JetBrains. Режим доступа: https://www.jetbrains.com/student/

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.