ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Заведующий выпускающей кафедрой

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Замышляева А. А.
Пользователь: zamyshliaevaaa
Дата подписания: 10.07.2024

А. А. Замышляева

РАБОЧАЯ ПРОГРАММА

дисциплины 1.Ф.П1.03 Криптографические протоколы
для направления 01.03.02 Прикладная математика и информатика
уровень Бакалавриат
профиль подготовки Математические методы обеспечения безопасности программных систем
форма обучения очная
кафедра-разработчик Прикладная математика и программирование

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 01.03.02 Прикладная математика и информатика, утверждённым приказом Минобрнауки от 10.01.2018 № 9

Зав.кафедрой разработчика,
д.физ.-мат.н., проф.

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Замышляева А. А.
Пользователь: zamyshliaevaaa
Дата подписания: 10.07.2024

А. А. Замышляева

Разработчик программы,
д.физ.-мат.н., доц., профессор

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Зюляркина Н. Д.
Пользователь: ziuliarkinand
Дата подписания: 04.07.2024

Н. Д. Зюляркина

Челябинск

1. Цели и задачи дисциплины

Целью изучения дисциплины является изучение студентами основных видов современных криптографических протоколов, методов их анализа и оценки стойкости, основных сфер практического применения и особенностей реализации. Задачами дисциплины являются: - ознакомление студентов со структурой современных сложных криптосистем, основными классами криптографических протоколов; - обзор методов анализа стойкости криптографических протоколов и средств криптографической защиты информации, в которых они реализуются; - изучение основных нормативно-технических документов, регламенти-рующих применение криптографических методов защиты информации, а также проектирование, разработку и применение средств криптографической защиты информации.

Краткое содержание дисциплины

В рамках данной дисциплины исследуются основные виды криптографических протоколов, различные типы атак на используемые протоколы и методы защиты от них. Кроме этого изучаются нормативно-технических документы, регламентирующие проектирование, разработку и применение средств крипто-графической защиты информации..

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
ПК-6 Способен использовать математические методы при проектировании и разработке алгоритмических и программных решений в области обеспечения безопасности и защиты программных систем.	Знает: различные виды криптографических протоколов поддержки сеанса, в том числе протоколы идентификации и аутентификации Имеет практический опыт: реализации известных криптографических протоколов в задачах обеспечения безопасности и защиты информации

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Криптографические методы защиты информации	Не предусмотрены

Требования к «входным» знаниям, умениям, навыкам студента, необходимым при освоении данной дисциплины и приобретенным в результате освоения предшествующих дисциплин:

Дисциплина	Требования
Криптографические методы защиты информации	Знает: основные понятия и задачи криптографии, математические модели криптографических систем; основные виды средств криптографической защиты информации (СКЗИ), включая блочные и поточные системы

	шифрования, криптографические системы с открытым ключом; национальные стандарты Российской Федерации в области криптографической защиты информации и сферы их применения Умеет: использовать систему криптографической защиты информации (СКЗИ) для решения задач профессиональной деятельности.

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 4 з.е., 144 ч., 82,5 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		8
Общая трудоёмкость дисциплины	144	144
Аудиторные занятия:	72	72
Лекции (Л)	24	24
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	24	24
Лабораторные работы (ЛР)	24	24
Самостоятельная работа (СРС)	61,5	61,5
Подготовка к экзамену	10	10
Разработка программ, реализующих различные криптографические протоколы.	11,5	11.5
Подготовка к практическим занятиям, выполнение домашних заданий.	40	40
Консультации и промежуточная аттестация	10,5	10,5
Вид контроля (зачет, диф.зачет, экзамен)	-	экзамен

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Основные понятия	4	2	2	0
2	Схемы цифровой подписи	14	2	6	6
3	Протоколы идентификации	14	4	4	6
4	Протоколы распределения ключей	20	6	8	6
5	Протоколы открытых сделок	14	4	4	6
6	Прикладные протоколы	4	4	0	0
7	Нормативные документы в области криптографических протоколов.	2	2	0	0

5.1. Лекции

№	№	Наименование или краткое содержание лекционного занятия	Кол-

лекции	раздела		во часов
1	1	Понятие криптографического протокола. Роль криптографических протоколов в системах защиты информации. Свойства протоколов, характеризующие их безопасность. Основные виды уязвимостей. Подходы к классификации криптографических протоколов. Подходы к моделированию криптографических протоколов. Понятие уязвимости и атаки на криптографический протокол. Использование симметричных и асимметричных шифрсистем для построения криптографических протоколов. Примеры. Основные подходы к автоматизации анализа протоколов.	2
2	2	Схемы цифровой подписи. Схемы цифровой подписи на основе симметричных и асимметричных шифрсистем. Стандарты США и России электронной цифровой подписи. Одноразовые подписи. Схемы конфиденциальной цифровой подписи и подписи вслепую. Подписи с обнаружением подделки.	2
3	3	Протоколы идентификации на основе паролей, протоколы “рукопожатия” и типа «запрос-ответ». Идентификация с использованием систем открытого шифрования.	2
4	3	Понятие протоколов интерактивного доказательства и доказательства знания. Протоколы идентификации на основе протоколов доказательства знания с нулевым разглашением	2
5	4	Схемы предварительного распределения ключей Блома и на основе пересечений множеств. Протокол открытого распределения ключей Диффи-Хэллмана и способы его защиты от атаки «противник в середине». Аутентифицированные протоколы открытого распределения ключей.	4
6	4	Групповые протоколы. Протоколы разделения секрета и распределения ключей для телеконференции.	2
7	5	Протоколы битовых обязательств и их свойства. Протоколы подбрасывания монеты и “игры в покер” по телефону.	2
8	5	Протоколы электронного голосования. Протокол использования электронных денег	2
15	6	Построение семейства протоколов KriptoKnight на основе базовых протоколов взаимной аутентификации и распределения ключей.	2
16	6	Особенности построения семейства протоколов IPsec. Протоколы Oakley, ISAKMP, IKE.	2
18	7	Протоколы SKIP, SSL/TLS и особенности их реализации.	2

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	1	Примеры протоколов на основе симметричных и асимметричных криптографических систем.	2
2	2	Примеры схем цифровых подписей. Контрольная работа "Цифровые подписи"	6
3	3	Протоколы «рукопожатия» и идентификации типа «запрос-ответ» с криптографической терминологией Протоколы доказательства знания с нулевым разглашением	3
4	3	Контрольная работа "Игровые протоколы"	1
5	4	Протоколы генерации и передачи ключей для симметричных шифрсистем. Протоколы генерации и передачи ключей для асимметричных шифрсистем.	4

		Протоколы разделения секрета	
6	4	Контрольная работа "Схемы предварительного распределения ключей".	2
7	4	Контрольная работа "Схемы разделения секрета "	2
8	5	Примеры прикладных протоколов (протоколы заключения сделок, платежных систем, сертифицированная электронная почта, голосования и др.)	4

5.3. Лабораторные работы

№ занятия	№ раздела	Наименование или краткое содержание лабораторной работы	Кол-во часов
1	2	Исследование хэш-функций, применяемых в схемах цифровой подписи Генерация ключей и вычисление подписи Фиата-Шамира. Проверка подписи Генерация ключей и вычисление подписи Эль-Гамаля. Проверка подписи	6
2	3	Протоколы с нулевым разглашением на основе задач о раскраске графа и поиска гамильтонова цикла	6
3	4	Протоколы предварительного распределения ключей (схема Блома и KDP-схемы). Схемы разделения секрета (групповая, Шамира, Миньотта, Блэкли, Карнина)	6
4	5	Протоколы привязки к биту (Гольдвассер-Микали, на основе циклических групп) Протоколы ментального покера	6

5.4. Самостоятельная работа студента

Выполнение СРС			
Подвид СРС	Список литературы (с указанием разделов, глав, страниц) / ссылка на ресурс	Семестр	Кол-во часов
Подготовка к экзамену	Музыкантский А.И., Фурин В.В. Лекции по криптографии [Электронный ресурс] / -- Московский центр непрерывного математического образования, 2013 — 68 с. http://e.lanbook.com/	8	10
Разработка программ, реализующих различные криптографические протоколы.	Музыкантский А.И., Фурин В.В. Лекции по криптографии [Электронный ресурс] / -- Московский центр непрерывного математического образования, 2013 — 68 с. http://e.lanbook.com/	8	11,5
Подготовка к практическим занятиям, выполнение домашних заданий.	Музыкантский А.И., Фурин В.В. Лекции по криптографии [Электронный ресурс] / -- Московский центр непрерывного математического образования, 2013 — 68 с. http://e.lanbook.com/	8	40

6. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации

Контроль качества освоения образовательной программы осуществляется в соответствии с Положением о балльно-рейтинговой системе оценивания результатов учебной деятельности обучающихся.

6.1. Контрольные мероприятия (КМ)

№ КМ	Се-местр	Вид контроля	Название контрольного мероприятия	Вес	Макс. балл	Порядок начисления баллов	Учи-тыва-ется в ПА
1	8	Текущий контроль	Контрольная работа "Игровые протоколы"	10	5	5 баллов - все задания решены 4 балла - решены все задания с мелкими недочетами 3 балла - в решении имеются значительные ошибки 2 бала - имеется большое количество существенных ошибок 1 балл - имеются намеки на решение	экзамен
2	8	Текущий контроль	Контрольная работа "Цифровые подписи"	10	5	5 баллов - все задания решены 4 балла - решены все задания с мелкими недочетами 3 балла - в решении имеются значительные ошибки 2 бала - имеется большое количество существенных ошибок 1 балл - имеются намеки на решение	экзамен
3	8	Текущий контроль	Контрольная работа "Схемы предварительного распределения ключей"	15	5	5 баллов - все задания решены 4 балла - решены все задания с мелкими недочетами 3 балла - в решении имеются значительные ошибки 2 бала - имеется большое количество существенных ошибок 1 балл - имеются намеки на решение	экзамен
4	8	Проме-жуточная аттестация	Контрольная работа "Схемы разделения секрета"	-	5	15 баллов - все задания решены 4 балла - решены все задания с мелкими недочетами 3 балла - в решении имеются значительные ошибки 2 бала - имеется большое количество существенных ошибок 1 балл - имеются намеки на решение	экзамен
5	8	Текущий контроль	Контрольная работа "Хэш-функции"	5	5	5 баллов - все задания решены 4 балла - решены все задания с мелкими недочетами 3 балла - в решении имеются значительные ошибки 2 бала - имеется большое количество существенных ошибок 1 балл - имеются намеки на решение	экзамен
6	8	Текущий контроль	Конспект лекций	3	10	10 баллов - конспект представлен в полном объёме 6-9 баллов - имеется около3/4 от всего объёма лекций 1-5 баллов - имеется 1/2 от всего объёма лекций 0 баллов - имеется менее половины объёма всех лекций	экзамен
7	8	Проме-жуточная аттестация	Экзамен	-	40	40 баллов - задача решена правильно 30-39 баллов -в решение есть неточности и незначительные ошибки	экзамен

						20-29 баллов - общий ход решения верен, но имеются серьёзные недочёты 10-19 балла - в решении присутствует ряд серьёзных ошибок 1-9 балл - есть некоторый намёк на решение 0 баллов - задача не решалась	

6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
экзамен	Экзамен проводится в форме устного опроса. В аудитории, где проводится экзамен, должно одновременно присутствовать не более 6-8 студентов. Каждому студенту задается по одному вопросу или заданию из каждой темы, выносимой на экзамен. При неправильном ответе студенту могут быть заданы уточняющие или новые вопросы из этой темы. Тема считается освоенной, если студент смог ответить на 2 вопроса, заданных по этой теме, и решить одну задачу.	В соответствии с пп. 2.5, 2.6 Положения

6.3. Паспорт фонда оценочных средств

Компетенции	Результаты обучения	№ КМ						
		1	2	3	4	5	6	7
ПК-6	Знает: различные виды криптографических протоколов поддержки сеанса, в том числе протоколы идентификации и аутентификации	+	+	+	+	+	+	+
ПК-6	Имеет практический опыт: реализации известных криптографических протоколов в задачах обеспечения безопасности и защиты информации	+	+	+	+	+		+

Типовые контрольные задания по каждому мероприятию находятся в приложениях.

7. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

Не предусмотрена

б) дополнительная литература:

Не предусмотрена

в) отечественные и зарубежные журналы по дисциплине, имеющиеся в библиотеке:

Не предусмотрены

г) методические указания для студентов по освоению дисциплины:

1. Зюляркина Н. Д. Криптографические методы защиты информации. Методические указания по проведению практических занятий

из них: учебно-методическое обеспечение самостоятельной работы студента:

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Основная литература	Электронно-библиотечная система издательства Лань	Музыкантский А.И., Фурин В.В. Лекции по криптографии [Электронный ресурс] / -- Московский центр непрерывного математического образования, 2013 — 68 с. http://e.lanbook.com/
2	Дополнительная литература	Электронно-библиотечная система издательства Лань	Рябко, Б.Я. Основы современной криптографии и стеганографии. [Электронный ресурс] / Б.Я. Рябко, А.Н. Фионов. — Электрон. дан. — М. : Горячая линия-Телеком, 2013. — 232 с. http://e.lanbook.com/

Перечень используемого программного обеспечения:

Нет

Перечень используемых профессиональных баз данных и информационных справочных систем:

Нет

8. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Лекции	912 (3б)	Комплект компьютерного оборудования, LCD Проектор, Экран проекционный, настенные стенды по защите информации (5 шт.), программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozila Firefox, Консультант+.
Практические занятия и семинары	913 (3б)	Комплект компьютерного оборудования; Локальная вычислительная сеть; Коммутатор, Программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozila Firefox, Консультант+; Локальные СЗИ: Secret Net 6.5 (автономный вариант), Страж 3.0; Межсетевые экраны: ViPNet Custom 3.1, User Gate 5.2