ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Руководитель специальности

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Соколов А. Н.
Пользователь: sokolovan
Дата подписания: 25.05.2022

А. Н. Соколов

РАБОЧАЯ ПРОГРАММА

дисциплины 1.О.41 Криптографические протоколы
для специальности 10.05.03 Информационная безопасность автоматизированных систем
уровень Специалитет
форма обучения очная
кафедра-разработчик Защита информации

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утверждённым приказом Минобрнауки от 26.11.2020 № 1457

Зав.кафедрой разработчика,
к.техн.н., доц.

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Соколов А. Н.
Пользователь: sokolovan
Дата подписания: 25.05.2022

А. Н. Соколов

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

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Зюляркина Н. Д.
Пользователь: ziuliarkinand
Дата подписания: 23.05.2022

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
ОПК-10 Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	Знает: предназначение криптографических протоколов в реализации политик информационной безопасности; область применения криптографических протоколов в системе защиты автоматизированных систем Умеет: производить вычисления в алгебраических структурах (группах, кольцах и полях); применять теоретико-графовые и теоретико-множественные методы при реализации протоколов; производить аудит результатов выполненного протокола Имеет практический опыт: применения криптографических протоколов при решении задач профессиональной деятельности

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
1.О.31 Методы и средства криптографической 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
1.О.31 Методы и средства криптографической 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, криптографические хеш-функции и криптографические протоколы; 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 Имеет практический опыт:

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 3 з.е., 108 ч., 54,25 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		8
Общая трудоёмкость дисциплины	108	108
Аудиторные занятия:	48	48
Лекции (Л)	24	24
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	24	24
Лабораторные работы (ЛР)	0	0
Самостоятельная работа (СРС)	53,75	53,75
с применением дистанционных образовательных технологий	0	
Подготовка к практическим занятиям, выполнение домашних заданий.	40	40
Разработка программ, реализующих различные криптографические протоколы.	13,75	13.75
Консультации и промежуточная аттестация	6,25	6,25
Вид контроля (зачет, диф.зачет, экзамен)	-	зачет

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	8	2	6	0
3	Протоколы идентификации	8	4	4	0
4	Протоколы распределения ключей	14	6	8	0
5	Протоколы открытых сделок	8	4	4	0
6	Прикладные протоколы	4	4	0	0
7	Нормативные документы в области криптографических протоколов.	2	2	0	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-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

№	№	Наименование или краткое содержание практического занятия, семинара	Кол-

занятия	раздела		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. Протоколы разделения секрета	4
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

Не предусмотрены

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 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
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	13,75

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-</br>

							ется в ПА
1	8	Текущий контроль	Контрольная работа "Игровые протоколы"	1	10	10 баллов - задача решена правильно 8-9 баллов -в решение есть неточности и незначительные ошибки 6-7 баллов - общий ход решения верен, но имеются серьёзные недочёты 3-5 баллов - в решении присутствует ряд серьёзных ошибок 1-2 баллов - есть некоторый намёк на решение 0 баллов - задача не решалась	зачет
2	8	Текущий контроль	Контрольная работа "Цифровые подписи"	1	10	10 баллов - задача решена правильно 8-9 баллов -в решение есть неточности и незначительные ошибки 6-7 баллов - общий ход решения верен, но имеются серьёзные недочёты 3-5 баллов - в решении присутствует ряд серьёзных ошибок 1-2 баллов - есть некоторый намёк на решение 0 баллов - задача не решалась	зачет
3	8	Текущий контроль	Контрольная работа "Схемы предварительного распределения ключей"	1	10	10 баллов - задача решена правильно 8-9 баллов -в решение есть неточности и незначительные ошибки 6-7 баллов - общий ход решения верен, но имеются серьёзные недочёты 3-5 баллов - в решении присутствует ряд серьёзных ошибок 1-2 баллов - есть некоторый намёк на решение 0 баллов - задача не решалась	зачет
4	8	Текущий контроль	Контрольная работа "Схемы разделения секрета"	1	10	10 баллов - задача решена правильно 8-9 баллов -в решение есть неточности и незначительные ошибки 6-7 баллов - общий ход решения верен, но имеются серьёзные недочёты 3-5 баллов - в решении присутствует ряд серьёзных ошибок 1-2 баллов - есть некоторый намёк на решение 0 баллов - задача не решалась	зачет
5	8	Текущий контроль	Контрольная работа "Хэш-функции"	1	10	10 баллов - задача решена правильно 8-9 баллов -в решение есть неточности и незначительные ошибки 6-7 баллов - общий ход решения верен, но имеются серьёзные недочёты 3-5 баллов - в решении присутствует ряд серьёзных ошибок 1-2 баллов - есть некоторый намёк на решение 0 баллов - задача не решалась	зачет
6	8	Текущий контроль	Конспект лекций	1	10	10 баллов - конспект представлен в полном объёме 6-9 баллов - имеется около3/4 от всего	зачет

						объёма лекций 1-5 баллов - имеется 1/2 от всего объёма лекций 0 баллов - имеется менее половины объёма всех лекций	
7	8	Проме-жуточная аттестация	Зачёт	-	40	40 баллов - задача решена правильно 30-39 баллов -в решение есть неточности и незначительные ошибки 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	зачет

6.2. Процедура проведения, критерии оценивания

Не предусмотрены

6.3. Паспорт фонда оценочных средств

Компетенции	Результаты обучения	№ КМ						
		1	2	3	4	5	6	7
ОПК-10	Знает: предназначение криптографических протоколов в реализации политик информационной безопасности; область применения криптографических протоколов в системе защиты автоматизированных систем	+	+	+	+	+	+	+
ОПК-10	Умеет: производить вычисления в алгебраических структурах (группах, кольцах и полях); применять теоретико-графовые и теоретико-множественные методы при реализации протоколов; производить аудит результатов выполненного протокола	+	+	+	+	+		+
ОПК-10	Имеет практический опыт: применения криптографических протоколов при решении задач профессиональной деятельности			+	+			+

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
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
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+.