ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Директор института
Институт естественных и точных наук

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: 15.10.2021

А. А. Замышляева

РАБОЧАЯ ПРОГРАММА

дисциплины 1.Ф.П2.03 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: 15.10.2021

А. А. Замышляева

Разработчик программы,
старший преподаватель

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Ножкина Т. Г.
Пользователь: nozhkinatg
Дата подписания: 14.10.2021

Т. Г. Ножкина

СОГЛАСОВАНО

Руководитель образовательной программы
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: 15.10.2021

А. А. Замышляева

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, регламентирующих 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 криптографической 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
Теория информации и кодирования, Математические основы криптографии, 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
Теория информации и кодирования	Знает: способы формирования оптимальных кодов в системе передачи информации Умеет: Имеет практический опыт: оценки предельных

	возможностей информационных систем, оптимального кодирования и передачи сигналов
Математические основы криптографии	Знает: алгебраические структуры, лежащие в основе современных криптографических систем Умеет: использовать математические методы при создании криптографических спецификаций Имеет практический опыт:
Криптографические методы защиты информации	Знает: принципы построения криптографических алгоритмов, криптографические стандарты, основные подходы к реализации криптографических средств защиты информации Умеет: Имеет практический опыт: решения задач, связанных с распределением ключевой информации, шифрованием чувствительной информации и цифровой подписью сообщений

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
с применением дистанционных образовательных технологий	0	
Подготовка к контрольным работам	10	10
Подготовка отчётов по лабораторным работам.	20	20
Подготовка доклада	15	15
Подготовка к экзамену	16,5	16.5
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	8	2	2	4
2	Протоколы идентификации и аутентификации	18	6	6	6
3	Криптографические хеш-функции	8	4	4	0
4	Прикладные протоколы	38	12	12	14

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Криптографические протоколы, их свойства, основные определения.	2
2-3	2	Протоколы идентификации и аутентификации	4
4	2	Протокол привязки к биту. Игровые протоколы.	2
5-6	3	Криптографические хеш-функции.	4
7	4	Протокол ментального покера	2
8-9	4	Схемы цифровых подписей.	4
10	4	Протокол подписания контракта.	2
11-12	4	Протоколы электронного голосования.	4

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	1	Основные понятия. Простейшие криптографические протоколы. Примеры протоколов на основе симметричных и асимметричных криптографических систем.	2
2-3	2	Протоколы идентификации Фиата-Шамира, Шнорра, Окамото. Протокол GQ.	4
4	2	Протокол привязки к биту. Протоколы доказательства знания. Протокол Гольдвассера-Микали. Игровые протоколы.	2
5-6	3	Криптографические хеш функции. Доклады студентов.	4
7	4	Протокол ментального покера.	2
8	4	Контрольная работа 1.	2
9	4	Схемы цифровых подписей.	2
10	4	Протокол подписания контракта.	2
11	4	Протокол электронного голосования.	2
12	4	Контрольная работа 2.	2

5.3. Лабораторные работы

№ занятия	№ раздела	Наименование или краткое содержание лабораторной работы	Кол-во часов
1-2	1	Криптосистемы RSA и Эль-Гамаля.	4
3-4	2	Протоколы идентификации Фиата-Шамира, Шнорра, Окамото. Протокол GQ.	4
5	2	Протокол Гольдвассера-Микали.	2
6-7	4	Протокол ментального покера.	4
8-9	4	Протокол подписания контракта	4
10-11	4	Протокол электронного голосования	4
12	4	Прикладные протоколы. Защита отчётов по лабораторным работам.	2

5.4. Самостоятельная работа студента

Выполнение СРС			
Подвид СРС	Список литературы (с указанием	Семестр	Кол-

	разделов, глав, страниц) / ссылка на ресурс		во часов
Подготовка к контрольным работам	ЭУМД. осн. лит. п. 1, п. 2, п. 5.	8	10
Подготовка отчётов по лабораторным работам.	ЭУМД. осн. лит. п. 1, п. 2, п. 5.	8	20
Подготовка доклада	ЭУМД. осн. лит. п. 1, п. 2, п. 5., доп. лит. п.3., п. 4.	8	15
Подготовка к экзамену	ЭУМД. осн. лит. п. 1, п. 2, п. 5.	8	16,5

6. Текущий контроль успеваемости, промежуточная аттестация

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	КМ-1. Лабораторная работа № 1	5	4	Верно зашифровано в системе RSA - 1 балл; Верно зашифровано в сисамалтеме Эль-Гамаля - 1 балл; Верно расшифровано в системе RSA - 1 балл; Верно расшифровано в сисамалтеме Эль-Гамаля - 1 балл;	экзамен
2	8	Текущий контроль	КМ-2. Лабораторная работа № 2	5	5	Студент получает за каждый [1 - 4] верно реализованный протокол 1 балл; Верно оформил и представил отчёт - 1 балл.	экзамен
3	8	Текущий контроль	КМ-3. Лабораторная работа № 3	5	3	За каждое (1, 2) верно выполненное задание - 1 балл. Верно оформил и представил отчёт - 1 балл.	экзамен
4	8	Текущий контроль	КМ-4. Лабораторная работа № 4	10	4	Правильно задана криптографическая платформа - 1 балл; верно произведена раздача карт - 1 балл; верно даны ответы на все поставленные вопросы - 1 балл; верно оформил и представил отчёт - 1 балл.	экзамен
5	8	Текущий контроль	КМ-5. Лабораторная работа № 5	10	3	Верно сделана фаза привязки - 1 балл; верно сделана фаза раскрытия - 1 балл верно оформлен и представлен отчёт - 1 балл.	экзамен
6	8	Текущий контроль	КМ-6. Лабораторная работа № 6	15	7	1 балл за каждого из пятерых участников, верно передавших информацию в счётные комиссии; 1 балл - верно подведён итог	экзамен

						голосования; 1 балл - верно оформил и представил отчёт.	
7	8	Текущий контроль	КМ-7. Контрольная работа 1	15	6	Задача 1: верно задана криптографическая платформа - 1 балл; верно произведена раздача - 1 балл4 получены верные ответы на все поставленные вопросы - 1 балл. Задача 2 решена верно - 1 балл. Задача 3: верно решён пункт а) - 1 балл; верно решён пункт б) - 1 балл.	экзамен
8	8	Текущий контроль	КМ-8. Контрольная работа 2	15	7	Задача 1: верно решён пункт а) - 1 балл; верно решён пункт б) - 1 балл. Задача 2: верно решён пункт а) - 1 балл; верно решён пункт б) - 1 балл. Задача 3: 1 балл за верно поданную информацию в каждую из трёх комиссий.	экзамен
9	8	Текущий контроль	КМ-9. Доклад	10	5	Подготовлен доклад - 1 балл; Подготовлена презентация - 1 балл; Оформление презентации соответствует ГОСТ - 1 балл; Тема раскрыта - 1 балл; Доклад вызвал интерес у аудитории - 1 балл.	экзамен
10	8	Текущий контроль	КМ-10. Активная познавательная деятельность	10	72	На каждом из 36 занятий студент может получить 2 балла: Студент задает вопросы по докладу - 1 балл; Студент правильно отвечает на вопросы по докладу - 1 балл. В противном случае баллы не начисляются.	экзамен
11	8	Проме-жуточная аттестация	КМ-11. Опрос	1	4	Контрольное мероприятие промежуточной аттестации проводится во время экзамена в виде устного опроса. Студенту задаются 4 вопроса из разных тем курса. Правильный ответ на вопрос - 1 балл; Неправильный ответ на вопрос - 0 баллов.	экзамен

6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
экзамен	На экзамене происходит оценивание учебной деятельности обучающихся по дисциплине на основе полученных оценок за контрольно-рейтинговые мероприятия текущего контроля.	В соответствии с пп. 2.5, 2.6 Положения

	Студент может улучшить свой рейтинг, пройдя контрольное мероприятие промежуточной аттестации, которое не является обязательным. Контрольное мероприятие промежуточной аттестации проводится во время экзамена в виде устного опроса. Студенту задаются 4 вопроса из разных тем курса. Студенту дается 30 минут на подготовку ответов. Затем студент озвучивает свои ответы.	

6.3. Оценочные материалы

Компетенции	Результаты обучения	№ КМ									
		1	2	3	4	5	6	7	8	9	10	11
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			+	+	+	+	+	+		+	+

Фонды оценочных средств по каждому контрольному 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	Рябко, Б. Я. Основы современной криптографии и стеганографии : монография / Б. Я. Рябко, А. Н. Фионов. — 2-е изд. — Москва : Горячая линия-Телеком, 2016. — 232 с. — ISBN 978-5-9912-0350-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111098 (дата обращения: 14.10.2021). — Режим доступа: для авториз. пользователей.

2	Основная литература	Электронно-библиотечная система издательства Лань	Аграновский, А. В. Практическая криптография: алгоритмы и их программирование : справочник / А. В. Аграновский, Р. А. Хади. — Москва : СОЛОН-Пресс, 2009. — 256 с. — ISBN 5-98003-002-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/13653 (дата обращения: 14.10.2021). — Режим доступа: для авториз. пользователей.
3	Дополнительная литература	Электронно-библиотечная система издательства Лань	Музыкантский, А. И. Лекции по криптографии : учебное пособие / А. И. Музыкантский, В. В. Фурин. — 2-е изд. — Москва : МЦНМО, 2013. — 68 с. — ISBN 978-5-4439-2075-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/56408 (дата обращения: 14.10.2021). — Режим доступа: для авториз. пользователей.
4	Дополнительная литература	Электронно-библиотечная система издательства Лань	Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401 (дата обращения: 30.09.2021). — Режим доступа: для авториз. пользователей.
5	Основная литература	Электронно-библиотечная система издательства Лань	Борисова, С. Н. Криптографические методы защиты информации: классическая криптография : учебное пособие / С. Н. Борисова. — Пенза : ПГУ, 2018. — 186 с. — ISBN 978-5-907102-51-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/162235 (дата обращения: 30.09.2021). — Режим доступа: для авториз. пользователей.

Перечень используемого программного обеспечения:

1. Microsoft-Office(бессрочно)
2. -Python(бессрочно)
3. Microsoft-Microsoft Imagine Premium (Windows Client, Windows Server, Visual Studio Professional, Visual Studio Premium, Windows Embedded, Visio, Project, OneNote, SQL Server, BizTalk Server, SharePoint Server)(04.08.2019)

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	336 (3б)	Проектор, компьютер, экран.
Лабораторные занятия	327 (3б)	Компьютеры, доска.
Практические занятия и семинары	332 (3б)	Проектор, компьютеры, экран.