


Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		



УТВЕРЖДЕНО

решением Ученого совета факультета математики,
информационных и авиационных технологий
от 16 июня 2020 г., протокол № 5/20

Председатель /М.А.Волков
(подпись, расшифровка подписи)
« 16 » июня 2020 г.

РАБОЧАЯ ПРОГРАММА

Дисциплина	Криптографические методы защиты информации
Факультет	Математики, информационных и авиационных технологий
Кафедра	Информационная безопасность и теория управления
Курс	4

Направление (специальность): 02.03.03 Математическое обеспечение и администрирование информационных систем

Направленность (профиль/специализация): Технология программирования

Форма обучения: очная

очная, заочная, очно-заочная (указать только те, которые реализуются)

Дата введения в учебный процесс УлГУ: « 01 » 09 2020 г.


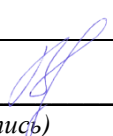
Программа актуализирована на заседании кафедры: протокол № от 20 г.


Программа актуализирована на заседании кафедры: протокол № от 20 г.

Программа актуализирована на заседании кафедры: протокол № от 20 г.

Сведения о разработчиках:

ФИО	Кафедра	Должность, ученая степень, звание
Андреев Александр Сергеевич	ИБиТУ	зав.каф. ИБиТУ, д.ф-м.н, профессор

СОГЛАСОВАНО	СОГЛАСОВАНО
Заведующий кафедрой информационной безопасности и теория управления, реализующей дисциплину	Заведующий выпускающей кафедрой информационных технологий
 <u> </u> / Андреев А.С. / (подпись) (Ф.И.О.)	 <u> </u> / Волков М.А. / (подпись) (Ф.И.О.)
« <u>15</u> » июня 2020 г.	« <u>16</u> » июня 2020 г.

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

1. ЦЕЛИ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины:

- приобретение общих представлений о криптографических методах и средствах обеспечения информационной безопасности;
- знакомство с важнейшими криптоалгоритмами, принципами их построения.

Задачи освоения дисциплины:

- освоение основных методов выбора алгоритмов для различных применений и оценки их качества;
- дать основы системного подхода к организации защиты информации; принципов синтеза и анализа шифров;
- дать основы математических методов, используемых в криптоанализе.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к вариативной части Блока 1 образовательной программы и читается в 7-м семестре студентам по направлению подготовки «Математическое обеспечение и администрирование информационных систем» очной формы обучения.

Для успешного освоения дисциплины необходимы знания основных фактов из базовых курсов: «Математический анализ», «Алгебра и геометрия», «Дискретная математика», «Теория вероятностей и математическая статистика», «Информатика и программирование». Предполагается также знакомство с одним из языков программирования высокого уровня (например, C/C++).


Для освоения дисциплины студент должен иметь следующие «входные» знания, умения, навыки и компетенции: вычислительные методы в алгебре и теории чисел.

Результаты освоения дисциплины будут необходимы для дальнейшего процесса обучения в рамках поэтапного формирования компетенций при изучении следующих специальных дисциплин: «Обнаружение вторжений и защита информации», а также для прохождения преддипломной практики и государственной итоговой аттестации.


3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины «Криптографические методы защиты информации» направлен на формирование следующих компетенций.

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
ОПК-2 – способен применять современный математический аппарат, связанный с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности	Знать: основные задачи и понятия криптографии; частотные характеристики открытых текстов и способы их применения к анализу простейших шифров замены и перестановки; алгоритмы проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в конечных циклических группах; Уметь: проводить вычисления в числовых и конечных

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

	<p>кольцах и полях с подстановками, многочленами, матрицами, в том числе с использованием компьютерных программ;</p> <p>Владеть:</p> <p>навыками эффективного вычисления в кольцах вычетов и в кольцах многочленов.</p>
<p>ПК-2 – способен использовать основные методы и средства автоматизации проектирования, реализации, испытаний и оценки качества при создании конкурентоспособного программного продукта и программных комплексов, а также способен использовать методы и средства автоматизации, связанные с сопровождением, администрированием и модернизацией программных продуктов и программных комплексов</p>	<p>Знать:</p> <p>основные виды симметричных и асимметричных криптографических алгоритмов; математические модели шифров и математические методы их исследования</p> <p>Уметь:</p> <p>эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах</p> <p>Владеть:</p> <p>навыками применения криптографических методов</p>
<p>ПК-3 – способен использовать знания направлений развития компьютеров с традиционной (нетрадиционной) архитектурой; современных системных программных средств; операционных систем, операционных и сетевых оболочек, сервисных программ; тенденции развития функций и архитектур проблемно-ориентированных программных систем и комплексов в профессиональной деятельности</p>	<p>Знать:</p> <p>требования к шифрам и основные характеристики шифров; модели шифров и математические методы их исследования;</p> <p>Уметь:</p> <p>корректно применять симметричные и асимметричные криптографические алгоритмы в программных системах и комплексах в профессиональной деятельности;</p> <p>Владеть:</p> <p>навыками применения криптографических методов</p>
<p>ПК-4 – способен использовать основные концептуальные положения функционального, логического, объектно-ориентированного и визуального направлений программирования, методы, способы и средства разработки программ в рамках этих направлений</p>	<p>Знать:</p> <p>требования к шифрам и основные характеристики шифров; модели шифров и математические методы их исследования;</p> <p>Уметь:</p> <p>корректно применять симметричные и асимметричные криптографические алгоритмы в программных системах и комплексах в профессиональной деятельности;</p> <p>Владеть:</p> <p>навыками применения криптографических методов</p>
<p>ПК-5 – способен использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования</p>	<p>Знать:</p> <p>требования к шифрам и основные характеристики шифров; модели шифров и математические методы их исследования;</p> <p>Уметь:</p> <p>корректно применять симметричные и асимметричные криптографические алгоритмы в программных</p>

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

	системах и комплексах в профессиональной деятельности; Владеть: навыками применения криптографических методов
--	---


4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего) 3.

4.2. Объем дисциплины по видам учебной работы:


Вид учебной работы	Количество часов (форма обучения - очная)			
	Всего по плану	В т.ч. по семестрам		
		5	6	7
Контактная работа обучающихся с преподавателем	54	-	-	54/54*
Аудиторные занятия:	54	-	-	54/54*
• Лекции	18	-	-	18/18*
• Практические и семинарские занятия	18	-	-	18/18*
• Лабораторные работы (лабораторный практикум)	18	-	-	18/18*
Самостоятельная работа	54	-	-	54
Форма текущего контроля знаний и контроля самостоятельной работы	-	-	-	Лабораторные работы, проверка решения задач
Курсовая работа	-	-	-	-
Экзамен	-	-	-	-
Всего часов по дисциплине	108	-	-	108
Виды промежуточной аттестации (экзамен, зачет)	-	-	-	Зачёт
Общая трудоемкость в зач. ед.	3	-	-	3

*В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий в таблице через слеш указывается количество часов работы ППС с обучающимися для проведения занятий в дистанционном формате с применением электронного обучения.

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

4.3. Содержание дисциплины. Распределение часов по темам и видам учебной работы:
Форма обучения очная

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	
Раздел 1. Математическая модель шифров							
1. Шифры замены и перестановки	16	2	2	4		8	Лабораторная работа. Домашние задания
2. Математические модели открытых текстов	8	2	2			4	Домашние задания
Раздел 2. Надежность шифров							
3. Совершенные шифры.	16	2	2	4		8	Лабораторная работа. Домашние задания
4. Вопросы имитостойкости шифров.	8	2	2			4	Домашние задания
5. Шифры, не распространяющие искажений.	8	2	2			4	Домашние задания
Раздел 3. Схемы разделения секрета							
6. Пороговые схемы разделения секрета.	16	2	2	4		8	Лабораторная работа. Домашние задания
7. Схемы разделения секрета с произвольной структурой доступа.	8	2	2			4	Домашние задания
Раздел 4. Блочные шифры							
8. Симметричные блочные шифры	20	2	2	6		10	Лабораторная работа. Домашние задания
9. Режимы симметричных блочных шифров	8	2	2			4	Домашние задания
Итого	108	18	18	18		54	

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Раздел 1. Математическая модель шифров

Тема 1. Шифры замены и перестановки

Шифр простой замены. Шифр сдвига. Методы взлома данного шифра. Аффинный шифр и методы его взлома. Преобразование биграмм аффинным шифром. Шифр замены с конечным ключом. Шифр Виженера. Криптоанализ шифра Виженера. Многопетлевые подстановки. Аффинный блочный шифр. Шифр Холла. Криптоанализ аффинного блочного шифра. Табличное гаммирование. Модульное гаммирование. Шифр Вернама. Шифр пропорциональной замены (шифр омофонов). Маршрутные перестановки. Криптоанализ шифров.

Тема 2. Математические модели открытых текстов

Детерминированная модель открытого текста. Вероятностная модель независимых символов алфавита. Вероятностная модель независимых биграмм. Вероятностная модель марковски зависимых символов. Критерии распознавания открытых текстов. Критерий на основе проверки гипотезы с использованием леммы Неймана-Пирсона. Критерий на основе запретных m -грамм.

Раздел 2. Надежность шифров


Тема 3. Совершенные шифры

Определение совершенного по Шеннону шифра. Эквивалентные условия. Необходимые условия совершенного по Шеннону шифра. Достаточное условие совершенного по Шеннону шифра. Теорема Шеннона. Критерий совершенных шифров в классе шифров с равномерным распределением вероятностей на множестве ключей. Пример совершенного неэндоморфного шифра с равномерным распределением на множестве ключей. Пример совершенного эндоморфного шифра с неравномерным распределением на множестве ключей. Пример совершенного неэндоморфного шифра с неравномерным распределением на множестве ключей. Примеры совершенных шифров с условиями $|X|=|Y|=|K|$, $|X|<|Y|=|K|$, $|X|=|Y|<|K|$, $|X|<|Y|<|K|$. $(k|y)$ -совершенные шифры: определение, эквивалентные условия. Необходимые и достаточные условия $(k|y)$ -совершенных шифров. Необходимые и достаточные условия одновременно совершенных и $(k|y)$ -совершенных шифров. Примеры $(k|y)$ -совершенных шифров с условиями $|X|=|Y|>|K|$, $|X|=|Y|=|K|$, $|X|=|Y|<|K|$. Примеры одновременно совершенного и $(k|y)$ -совершенного шифра с условиями $|X|=|Y|=|K|$, $|X|=|Y|<|K|$. Математические модели шифра замены с ограниченным и неограниченным ключом. Шифрвеличины и шифробозначения. Опорный шифр шифра замены. Степень опорного шифра. Случайный и детерминированный генераторы ключевого потока. Шифр замены с неограниченным ключом. Шифр замены с ограниченным ключом. Совершенные шифры замены. Определение совершенного шифра замены, эквивалентные условия. Несовершенство в общем случае шифра замены с ограниченным ключом. Достаточные условия совершенного шифра замены с неограниченным ключом. Критерий совершенности шифра замены с неограниченным ключом в классе эндоморфных шифров. Критерий совершенности шифра замены с неограниченным ключом в классе шифров с равномерным распределением на множестве ключей.

Тема 4. Вопросы имитостойкости шифров.

Подмена зашифрованного сообщения. Имитация зашифрованного сообщения. Имитостойкость шифра. Нижние оценки вероятности имитации и подмены сообщения. Примеры совершенных имитостойких шифров.

Тема 5. Шифры, не распространяющие искажений

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

Шифры, не распространяющие искажений типа замены знаков. Метрика Хэмминга на открытых и шифрованных текстах. Определение шифра, не распространяющего искажений типа замены знаков. Эквивалентные условия шифра, не распространяющего искажений типа замены знаков. Понятие изометрии. Теорема А.А.Маркова. Шифры, не распространяющие искажений типа пропуска (вставки) знаков. Определение шифра, не распространяющего искажений типа пропуска знаков. Эквивалентные условия шифра, не распространяющего искажений типа пропуска знаков. Критерий шифра, не распространяющего искажений типа пропуска знаков, в классе эндоморфных шифров.

Раздел 3. Схемы разделения секрета

Тема 6. Пороговые схемы разделения секрета

Понятие (n,t) пороговой схемы разделения секрета. Пример (n,n) пороговой схемы. Схема разделения секрета на основе решения СЛАУ. Схема разделения секрета Шамира. Проверяемая схема разделения секрета Фельдмана-Шамира. Совершенная проверяемая схема разделения секрета Педерсона-Шамира. Схемы разделения секрета на основе n -разрядных равновесных двоичных кодов.

Тема 7. Схемы разделения секрета с произвольной структурой доступа

Схемы разделения секрета для произвольных структур доступа: основные понятия. Схема Бенало-Лейхтера. Схема Ито-Саито-Нишизеки.

Раздел 4. Блочные шифры

Тема 8. Симметричные блочные шифры

Итеративные блочные шифры. Понятие раундовой функции, раундового ключа. Условия, обеспечивающие обратимость итеративного блочного шифра. Построение цикловой функции. Входное и выходное отображения. Слабые ключи итеративного блочного шифра. Определение шифра Фейстеля. Функция усложнения шифра Фейстеля. Условия, обеспечивающие обратимость шифра Фейстеля. Примеры итеративных блочных шифров. Шифры “Магма” и “Кузнечик” из ГОСТ Р 34.12-2015. Шифр AES.

Тема 9. Режимы использования блочных шифров.

Режим электронной кодовой книги. Режим сцепления блоков. Режим гаммирования с обратной связью по шифртексту. Режим гаммирования. Режим выработки имитовставки. Свойства данных режимов.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ


Раздел 1. Математическая модель шифров

Тема 1. Шифры замены и перестановки

Шифр простой замены. Шифр сдвига. Методы взлома данного шифра. Аффинный шифр и методы его взлома. Преобразование биграмм аффинным шифром. Шифр замены с конечным ключом. Шифр Виженера. Криптоанализ шифра Виженера. Многопетлевые подстановки. Аффинный блочный шифр. Шифр Холла. Криптоанализ аффинного блочного шифра. Табличное гаммирование. Модульное гаммирование. Шифр Вернама. Шифр пропорциональной замены (шифр омофонов). Маршрутные перестановки. Криптоанализ шифров.

Тема 2. Математические модели открытых текстов

Детерминированная модель открытого текста. Вероятностная модель независимых символов алфавита. Вероятностная модель независимых биграмм. Вероятностная модель марковски зависимых символов. Критерии распознавания открытых текстов. Критерий на основе проверки гипотезы с использованием леммы Неймана-Пирсона. Критерий на основе запретных m -грамм.

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

Раздел 2. Надежность шифров

Тема 3. Совершенные шифры

Определение совершенного по Шеннону шифра. Эквивалентные условия. Необходимые условия совершенного по Шеннону шифра. Достаточное условие совершенного по Шеннону шифра. Теорема Шеннона. Критерий совершенных шифров в классе шифров с равномерным распределением вероятностей на множестве ключей. Пример совершенного неэндоморфного шифра с равномерным распределением на множестве ключей. Пример совершенного эндоморфного шифра с неравномерным распределением на множестве ключей. Пример совершенного неэндоморфного шифра с неравномерным распределением на множестве ключей. Примеры совершенных шифров с условиями $|X|=|Y|=|K|$, $|X|<|Y|=|K|$, $|X|=|Y|<|K|$, $|X|<|Y|<|K|$. $(k|y)$ -совершенные шифры: определение, эквивалентные условия. Необходимые и достаточные условия $(k|y)$ -совершенных шифров. Необходимые и достаточные условия одновременно совершенных и $(k|y)$ -совершенных шифров. Примеры $(k|y)$ -совершенных шифров с условиями $|X|=|Y|>|K|$, $|X|=|Y|=|K|$, $|X|=|Y|<|K|$. Примеры одновременно совершенного и $(k|y)$ -совершенного шифра с условиями $|X|=|Y|=|K|$, $|X|=|Y|<|K|$. Математические модели шифра замены с ограниченным и неограниченным ключом. Шифрвеличины и шифробозначения. Опорный шифр шифра замены. Степень опорного шифра. Случайный и детерминированный генераторы ключевого потока. Шифр замены с неограниченным ключом. Шифр замены с ограниченным ключом. Совершенные шифры замены. Определение совершенного шифра замены, эквивалентные условия. Несовершенство в общем случае шифра замены с ограниченным ключом. Достаточные условия совершенного шифра замены с неограниченным ключом. Критерий совершенности шифра замены с неограниченным ключом в классе эндоморфных шифров. Критерий совершенности шифра замены с неограниченным ключом в классе шифров с равномерным распределением на множестве ключей.

Тема 4. Вопросы имитостойкости шифров.

Подмена шифрованного сообщения. Имитация шифрованного сообщения. Имитостойкость шифра. Нижние оценки вероятности имитации и подмены сообщения. Примеры совершенных имитостойких шифров.

Тема 5. Шифры, не распространяющие искажений

Шифры, не распространяющие искажений типа замены знаков. Метрика Хэмминга на открытых и шифрованных текстах. Определение шифра, не распространяющего искажений типа замены знаков. Эквивалентные условия шифра, не распространяющего искажений типа замены знаков. Понятие изометрии. Теорема А.А.Маркова. Шифры, не распространяющие искажений типа пропуска (вставки) знаков. Определение шифра, не распространяющего искажений типа пропуска знаков. Эквивалентные условия шифра, не распространяющего искажений типа пропуска знаков. Критерий шифра, не распространяющего искажений типа пропуска знаков, в классе эндоморфных шифров.


Раздел 3. Схемы разделения секрета

Тема 6. Пороговые схемы разделения секрета

Понятие (n,t) пороговой схемы разделения секрета. Пример (n,n) пороговой схемы. Схема разделения секрета на основе решения СЛАУ. Схема разделения секрета Шамира. Проверяемая схема разделения секрета Фельдмана-Шамира. Совершенная проверяемая схема разделения секрета Педерсона-Шамира. Схемы разделения секрета на основе n -разрядных равновесных двоичных кодов.

Тема 7. Схемы разделения секрета с произвольной структурой доступа

Схемы разделения секрета для произвольных структур доступа: основные понятия. Схема Бенало-Лейхтера. Схема Ито-Саито-Нишизеки.

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

Раздел 4. Блочные шифры

Тема 8. Симметричные блочные шифры

Итеративные блочные шифры. Понятие раундовой функции, раундового ключа. Условия, обеспечивающие обратимость итеративного блочного шифра. Построение цикловой функции. Входное и выходное отображения. Слабые ключи итеративного блочного шифра. Определение шифра Фейстеля. Функция усложнения шифра Фейстеля. Условия, обеспечивающие обратимость шифра Фейстеля. Примеры итеративных блочных шифров. Шифры “Магма” и “Кузнечик” из ГОСТ Р 34.12-2015. Шифр AES.

Тема 9. Режимы использования блочных шифров.

Режим электронной кодовой книги. Режим сцепления блоков. Режим гаммирования с обратной связью по шифртексту. Режим гаммирования. Режим выработки имитовставки. Свойства данных режимов.

7. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)

Полные задания для лабораторных работ приводятся в учебно-методическом пособии: Аминаров А. В. Лабораторный практикум по математическим методам защиты информации : учеб.-метод. указания для спец. "Компьютерная безопасность, "Математическое обеспечение и администрирование информационных систем" / А. В. Аминаров, А. М. Иванцов, С. М. Рацев. Ульяновск : УлГУ, 2016. 55 с.

Лабораторные работы проводятся в интерактивной форме, а именно, используются: диалоговое обучение, в ходе которого осуществляется взаимодействие между студентом и преподавателем, между самими студентами, группами студентов; элементы деловых игр, «мозговой штурм» или дискуссии по рассматриваемым вопросам.

Раздел 1. Математическая модель шифров

Тема 1. Шифры замены и перестановки

Цель работы: разработать криптографическую защиту информации, содержащейся в текстовом (двоичном) файле данных, с помощью алгоритма шифрования, указанного в варианте.


Задание.

1. Разработать алгоритмы шифрования и расшифрования открытого текста из алфавита $A=Z_n$ на заданном ключе с помощью метода, указанного в варианте.
2. Определить алфавит A криптосистемы (открытого текста и шифртекста). Если алфавит A не задан в варианте, выбрать его самостоятельно, так, чтобы он включал в себя символы используемого в примере открытого текста. Например, русский, английский, ASCII. Поставить символам исходного алфавита A в соответствие символы из алфавита Z_n (n – основание алфавита).
3. Написать функцию генерации случайных ключей шифра, оценить размерность ключевого пространства.
4. Написать функцию, реализующую шифрование на заданном ключе открытого текста, состоящего из символов заданного алфавита. Открытый текст, ключ и шифртекст должны быть представлены отдельными файлами.
5. Написать функцию для реализации алгоритма расшифрования полученного шифрованного файла при известном ключе.

Методические указания: основное внимание должно быть уделено освоению классических шифров.

Раздел 2. Надежность шифров

Тема 3. Совершенные шифры

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

Цель работы: ознакомиться с шифрованием и расшифрованием информации при помощи n -разрядного скремблера.

Задание.

1. Написать функцию генерации ключей шифра с помощью n -разрядного скремблера (значение n зависит от степени многочлена, указанного в варианте).
2. Написать функцию, реализующую шифрование на заданном ключе открытого текста, состоящего из символов алфавита Z_2 .
3. Написать функцию для реализации алгоритма расшифрования полученного зашифрованного файла при известном ключе.

Методические указания: основное внимание должно быть уделено освоению работы n -разрядного скремблера.

Раздел 3. Схемы разделения секрета

Тема 6. Пороговые схемы разделения секрета

Цель работы: изучение (n, t) -пороговых схем разделения секрета.

Задание. Реализовать схему разделения секрета в соответствии с индивидуальным вариантом. Программа должна уметь как разделять секрет s на n участников в соответствии с порогом t , так и восстанавливать его.

Варианты заданий:

1. Схема разделения секрета Шамира.
2. Схема разделения секрета на основе равновесных двоичных кодов.
3. Схема разделения секрета на основе китайской теоремы об остатках.

Методические указания: основное внимание должно быть уделено освоению принципов построения схем разделения секрета.

Раздел 4. Блочные шифры

Тема 8. Симметричные блочные шифры

Цель работы: ознакомиться с шифрованием и расшифрованием информации при помощи алгоритма “Магма” из ГОСТ Р 34.12-2015.

Задание. Реализовать шифр “Магма” из ГОСТ Р 34.12-2015 и основные режимы шифрования.

Методические указания: основное внимание должно быть уделено освоению шифра “Магма” из ГОСТ Р 34.12-2015 и основных режимов шифрования.

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

Не предусмотрено учебным планом.


9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ

Математические модели открытого текста

1. Детерминированная модель открытого текста.
2. Вероятностные модели открытого текста: модель независимых символов алфавита, модель независимых биграмм, модель марковски зависимых букв.

Шифры замены и перестановки

3. Одноалфавитные шифры замены: шифр простой замены, шифр сдвига. Методы взлома данных шифров.
4. Одноалфавитные шифры замены: аффинный шифр, преобразование биграмм аффинным шифром. Методы взлома данных шифров.
5. Многоалфавитные шифры замены. Шифр Виженера. Криптоанализ шифра Виженера.
6. Многоалфавитные шифры замены: многопетлевые подстановки, аффинный блочный шифр, шифр Холла. Криптоанализ аффинного блочного шифра.

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

7. Многоалфавитные шифры замены: табличное гаммирование, модульное гаммирование. Шифр Вернама.

8. Многоалфавитные шифры замены. Шифр пропорциональной замены (шифр омофонов).

Математическая модель шифра

9. Алгебраическая и вероятностная модели шифров.

10. Математическая модель некоторых шифров: шифр простой замены, шифр сдвига, аффинный шифр, шифр замены с конечным ключом, шифр Виженера, шифр перестановки.

Надежность шифров

11. Определение совершенного по Шеннону шифра. Эквивалентные условия. Необходимые условия совершенного по Шеннону шифра.

12. Достаточное условие совершенного по Шеннону шифра. Теорема Шеннона.

13. Критерий совершенных шифров в классе шифров с равномерным распределением вероятностей на множестве ключей.

14. $(k|y)$ -совершенные шифры: определение, эквивалентные условия.

15. Необходимые и достаточные условия $(k|y)$ -совершенных шифров.

Математическая модель шифра замены с ограниченным и неограниченным ключом

16. Понятие опорного шифра, степени опорного шифра. Случайный и детерминированный генераторы ключевого потока. Примеры генераторов.

17. Определение шифра замены с ограниченным и неограниченным ключом.

18. Определение совершенного шифра замены, эквивалентные условия. Несовершенство в общем случае шифра замены с ограниченным ключом.

19. Достаточные условия совершенного шифра замены с неограниченным ключом. Критерий совершенности шифра замены с неограниченным ключом.

Имитостойкие шифры

20. Понятие имитации сообщений. Определение вероятности $P_{\text{им}}$. Нижняя оценка для вероятности имитации сообщения. Критерий достижимости нижней оценки. Примеры шифров с достижимой нижней оценкой имитации сообщений.

21. Понятие подмены сообщений. Определение вероятности $P_{\text{подм}}$. Нижняя оценка для вероятности подмены сообщения. Критерий достижимости нижней оценки. Примеры шифров с достижимой нижней оценкой подмены сообщений.

22. Совершенные имитостойкие шифры замены с неограниченным ключом.

Шифры, не распространяющие искажений

23. Шифры, не распространяющие искажений типа замены знаков: определение, эквивалентные условия.

24. Понятие изометрии. Свойства изометрий.

25. Теорема А.А.Маркова. Примеры шифров, не распространяющих искажения типа замены знаков.

26. Шифры, не распространяющие искажений типа пропуска знаков: основные понятия.

27. Критерий для шифров, не распространяющих искажений типа пропуска знаков, в классе эндоморфных шифров.

28. Шифры, не распространяющие искажений типа вставки знаков

Схемы разделения секрета


29. Понятие (n, t) пороговой схемы разделения секрета. Пример (n, n) пороговой схемы. Схема разделения секрета на основе решения СЛАУ.

30. Схема разделения секрета Шамира.

31. Схемы разделения секрета на основе n -разрядных равновесных двоичных кодов.

32. Схема разделения секрета на основе китайской теоремы об остатках.

Симметричные блочные шифры

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

33. Итеративные блочные шифры. Обратимость итеративного блочного шифра.
34. Шифры Фейстеля и их обратимость.
35. Построение цикловой функции. Входное и выходное отображения.
36. Слабые ключи итеративного блочного шифра.
37. Режимы использования симметричных блочных шифров.
38. Шифр “Магма” из ГОСТ Р 34.12-2015.
39. Криптоанализ симметричных блочных шифров.

10. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ


Название разделов и тем	Вид самостоятельной работы	Объем в часах	Форма контроля
1. Шифры замены и перестановки	Проработка учебного материала, лабораторные работы, подготовка к сдаче экзамена, решение задач	8	Зачет, проверка лабораторных работ, проверка решения задач
2. Математические модели открытых текстов	Проработка учебного материала, подготовка к сдаче экзамена	4	Зачет, проверка решения задач
3. Совершенные шифры.	Проработка учебного материала, лабораторные работы, подготовка к сдаче экзамена, решение задач	8	Зачет, проверка лабораторных работ, проверка решения задач
4. Вопросы имитостойкости шифров.	Проработка учебного материала, подготовка к сдаче экзамена, решение задач	4	Зачет, проверка решения задач
5. Шифры, не распространяющие искажений.	Проработка учебного материала, подготовка к сдаче экзамена	4	Зачет, проверка решения задач
6. Пороговые схемы разделения секрета.	Проработка учебного материала, лабораторные работы, подготовка к сдаче экзамена, решение задач	8	Зачет, проверка лабораторных работ, проверка решения задач
7. Схемы разделения секрета с произвольной структурой доступа.	Проработка учебного материала, подготовка к сдаче экзамена, решение задач	4	Зачет, проверка решения задач
8. Симметричные блочные шифры	Проработка учебного материала, лабораторные работы, подготовка к сдаче экзамена	10	Зачет, проверка лабораторных работ
9. Режимы симметричных блочных шифров	Проработка учебного материала, подготовка к сдаче экзамена	4	Зачет, проверка решения задач

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы

Основная

1. Зубов А.Ю. Криптографические методы защиты информации. Совершенные шифры. М.: Гелиос АРВ, 2005. 192 с.
2. Рацеев С.М. Математические методы защиты информации : электронный учебный курс / С. М. Рацеев; УлГУ, ФМИАТ. - Ульяновск : УлГУ, 2018. — URL: <http://edu.ulsu.ru/courses/921/interface>

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

Дополнительная

1. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для академического бакалавриата / И. Н. Васильева. — Москва : Издательство Юрайт, 2019. — 349 с. — (Бакалавр. Академический курс). — ISBN 978-5-534-02883-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://biblio-online.ru/bcode/433610>
2. ГОСТ-Эксперт – единая база ГОСТов Российской Федерации для образования и промышленности:
 - 2.1. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. М.: Стандартинформ, 2012.
 - 2.2. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования. М.: Стандартинформ, 2013.

Учебно-методическая

1. Аминаров А. В. Лабораторный практикум по математическим методам защиты информации : учеб.-метод. указания для спец. "Компьютерная безопасность, "Математическое обеспечение и администрирование информационных систем" / А. В. Аминаров, А. М. Иванцов, С. М. Рацеев. Ульяновск : УлГУ, 2016. 55 с. -URL: <http://lib.ulsu.ru/MegaPro/Download/MObject/270>
2. Рацеев С.М. Методические указания для самостоятельной работы студентов по дисциплине «Криптографические методы защиты информации» для студентов направления подготовки 02.03.03 «Математическое обеспечение и администрирование информационных систем» / С. М. Рацеев; УлГУ, Фак. математики, информ. и авиац. технологий. - Ульяновск : УлГУ, 2019. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 176 КБ). - Текст : электронный. Режим доступа: <http://lib.ulsu.ru/MegaPro/Download/MObject/4687>

Согласовано:

И.Б. Биб-ро ИБ УлГУ
должность сотрудника научной библиотеки

ФИО

подпись

дата

Полина И.И. 08.06.2020

б) Программное обеспечение

Для образовательного процесса по данной дисциплине необходим стационарный класс ПК с установленным следующим программным обеспечением:

- операционная среда ОС Windows/Linux;
- системы программирования на языках Си/C++ (Code::Blocks).

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:


1.1. IPRbooks [Электронный ресурс]: электронно-библиотечная система / группа компаний Ай Пи Эр Медиа . - Электрон. дан. - Саратов , [2020]. - Режим доступа: <http://www.iprbookshop.ru>.

1.2. ЮРАЙТ [Электронный ресурс]: электронно-библиотечная система / ООО Электронное издательство ЮРАЙТ. - Электрон. дан. – Москва , [2020]. - Режим доступа: <https://www.biblio-online.ru>.

1.3. Консультант студента [Электронный ресурс]: электронно-библиотечная система / ООО Политехресурс. - Электрон. дан. – Москва, [2020]. - Режим доступа: <http://www.studentlibrary.ru/pages/catalogue.html>.

1.4. Лань [Электронный ресурс]: электронно-библиотечная система / ООО ЭБС Лань. - Электрон. дан. – С.-Петербург, [2020]. - Режим доступа: <https://e.lanbook.com>.

1.5. Znanium.com [Электронный ресурс]: электронно-библиотечная система / ООО Знаниум. - Электрон. дан. – Москва, [2020]. - Режим доступа: <http://znanium.com>.

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. /Компания «Консультант Плюс» - Электрон. дан. - Москва: КонсультантПлюс, [2020].

3. База данных периодических изданий [Электронный ресурс] : электронные журналы / ООО ИВИС. - Электрон. дан. - Москва, [2020]. - Режим доступа: <https://dlib.eastview.com/browse/udb/12>.

4. Национальная электронная библиотека [Электронный ресурс]: электронная библиотека. - Электрон. дан. – Москва, [2020]. - Режим доступа: <https://нэб.рф>.

5. Электронная библиотека диссертаций РГБ [Электронный ресурс]: электронная библиотека / ФГБУ РГБ. - Электрон. дан. – Москва, [2020]. - Режим доступа: <https://dvs.rsl.ru>.

6. ГОСТ-Эксперт - единая база ГОСТов Российской Федерации для образования и промышленности.

7. Федеральные информационно-образовательные порталы:

7.1. Информационная система Единое окно доступа к образовательным ресурсам. Режим доступа: <http://window.edu.ru>

7.2. Федеральный портал Российское образование. Режим доступа: <http://www.edu.ru>

8. Образовательные ресурсы УлГУ:

8.1. Электронная библиотека УлГУ. Режим доступа: <http://lib.ulsu.ru/MegaPro/Web>

8.2. Образовательный портал УлГУ. Режим доступа: <http://edu.ulsu.ru>

Согласовано:

зам. нач. УИТиТ

должность сотрудника УИТиТ

Киселева ДВ

ФИО

08.06.2020

подпись

дата


12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Аудитория -3/316. Аудитория для проведения лекционных, семинарских и практических занятий, текущего контроля и промежуточной аттестации, групповых и индивидуальных консультаций. Комплект переносного мультимедийного оборудования: ноутбук с выходом в Интернет, экран, проектор, Wi-Fi с доступом в Интернет, ЭИОС, ЭБС. 432017, Ульяновская область, г. Ульяновск, ул. Набережная реки Свияги, д. 106-3 корпус

Аудитория -3/118. Аудитория для проведения лабораторных и практических занятий, текущего контроля и промежуточной аттестации, групповых и индивидуальных консультаций. 15 компьютеров, Wi-Fi с доступом к сети «Интернет», ЭИОС, ЭБС. Проектор, экран. 432017, Ульяновская область, г. Ульяновск, ул. Набережная реки Свияги, д. 106-3 корпус

Аудитория -230. Аудитория для самостоятельной работы. Аудитория укомплектована ученической мебелью. 16 персональных компьютеров. 432017, Ульяновская область, г. Ульяновск, р-н Железнодорожный, ул. Набережная р. Свияги, № 106-1 корпус

Аудитория -237. Читальный зал научной библиотеки с зоной для самостоятельной работы. Аудитория укомплектована ученической мебелью. Компьютерная техника, телевизор, экран, проектор. Стол для лиц с ОВЗ. 432017, Ульяновская область, г. Ульяновск, р-н Железнодорожный, ул. Набережная р. Свияги, № 106-1 корпус.

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ


В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающимся) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических возможностей:

- для лиц с нарушением зрения: в форме электронного документа, индивидуальные консультации с привлечением тифлосурдопереводчика, индивидуальные задания и консультация;
- для лиц с нарушением слуха: в форме электронного документа, индивидуальные консультации с привлечением сурдопереводчика, индивидуальные задания и консультация;

для лиц с нарушением опорно-двигательного аппарата: в форме электронного документа, индивидуальные задания и консультация.

В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий, организация работы ППС с обучающимися с ОВЗ и инвалидами предусматривается в электронной информационно-образовательной среде с учетом их индивидуальных психофизических особенностей.

Разработчик

 / Андреев А.С. /
(подпись) (Ф.И.О.)