


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 » 06 2020 г., протокол № 5/20
Председатель / М.А. Волков /
(подпись, расшифровка подписи)
06 2020 г.

РАБОЧАЯ ПРОГРАММА

Дисциплина	Криптографические методы защиты информации
Факультет	Математики, информационных и авиационных технологий
Кафедра	Информационной безопасности и теории управления
Курс	4

Специальность: 10.05.03 «Информационная безопасность автоматизированных систем»
код направления (специальности), полное наименование

Специализация: «Безопасность открытых информационных систем»
полное наименование

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 № 12 от 12.05 2021 г.


Программа актуализирована на заседании кафедры: протокол № 13 от 11.05 2022 г.

Программа актуализирована на заседании кафедры: протокол № 12 от 12.04 2023 г.

Сведения о разработчиках:

ФИО	Кафедра	Должность, ученая степень, звание
Рацев Сергей Михайлович	ИБиТУ	профессор, д.ф-м.н, доцент

СОГЛАСОВАНО
Заведующий выпускающей кафедрой
 (Подпись) / <u>А.С. Андреев</u> / (Ф.И.О.) « <u>16</u> » <u>06</u> 20 <u>20</u> 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 базовой части цикла Б1 образовательной программы и читается в 7-м семестре студентам специальности «Информационная безопасность автоматизированных 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». 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: теоретико-числовые методы в криптографии, 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: «Криптографические протоколы и стандарты», «Методы алгебраической геометрии в криптографии», а также для прохождения учебной, производственной и преддипломной практик, государственной итоговой аттестации.


3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СОТНЕСЕННЫХ 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
ОК-6 – способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия	Владеть: криптографической терминологией
ОПК-1 – способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач	Уметь: применять математические методы исследования моделей шифров
ОПК-2 – способностью корректно применять при	Знать:

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

решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники	основные задачи и понятия криптографии; частотные характеристики открытых текстов и способы их применения к анализу простейших шифров замены и перестановки
ОПК-3 – способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности	Владеть: навыками использования ЭВМ в анализе простейших шифров
ОПК-5 – способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	Знать: основные задачи и понятия криптографии
ПК-1 – способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке	Владеть: криптографической терминологией
ПК-2 – способностью создавать и исследовать модели автоматизированных систем	Знать: модели шифров и математические методы их исследования Владеть: навыками математического моделирования в криптографии
ПК-3 – способностью проводить анализ защищенности автоматизированных систем	Знать: требования к шифрам и основные характеристики шифров; модели шифров и математические методы их исследования
ПК-5 – способностью проводить анализ рисков информационной безопасности автоматизированной системы	Знать: требования к шифрам и основные характеристики шифров
ПК-6 – способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	Знать: требования к шифрам и основные характеристики шифров
ПК-11 – способностью разрабатывать политику информационной безопасности автоматизированной системы	Знать: основные задачи и понятия криптографии
ПК-13 – способностью участвовать в проектировании средств защиты информации автоматизированной системы	Знать: требования к шифрам и основные характеристики шифров; типовые поточные и блочные шифры Уметь: эффективно использовать криптографические ме-

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


	тоды и средства защиты информации в автоматизированных системах Владеть: криптографической терминологией
ПК-14 – способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	Знать: требования к шифрам и основные характеристики шифров
ПК-15 – способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем	Знать: требования к шифрам и основные характеристики шифров
ПК-22 – способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	Уметь: эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах Владеть: криптографической терминологией
ПК-23 – способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	Знать: основные задачи и понятия криптографии; требования к шифрам и основные характеристики шифров; типовые поточные и блочные шифры
ПК-26 – способностью администрировать подсистему информационной безопасности автоматизированной системы	Знать: типовые шифры с открытыми ключами;
ПК-27 – способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	Знать: типовые шифры с открытыми ключами Владеть: навыками использования типовых криптографических алгоритмов; навыками использования ЭВМ в анализе простейших шифров

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего) 4.

4.2. Объем дисциплины по видам учебной работы:

Вид учебной работы	Количество часов (форма обучения - дневная)			
	Всего по плану	В т.ч. по семестрам		
			7	
Контактная работа обучающихся с преподавателем	54		54	


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

Аудиторные занятия:				
• Лекции	36		36	
• Практические и семинарские занятия				
• Лабораторные работы (лабораторный практикум)	18		18	
Самостоятельная работа	54		54	
Форма текущего контроля знаний и контроля самостоятельной работы			Лабораторные работы, проверка решения задач	
Курсовая работа				
Экзамен	36		36	
Всего часов по дисциплине	144		144	
Виды промежуточной аттестации (экзамен, зачет)	экзамен		экзамен	
Общая трудоемкость в зач. ед.	4		4	

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	12	4		2	2	6	Лабораторная работа. Домашние задания
2. Математические модели открытых текстов	4	2				2	
3. Математическая	4	2				2	

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

модель шифров							
Раздел 2. Надежность шифров							
4. Совершенные шифры.	24	8		4	4	12	Лабораторная работа. Домашние задания
5. Вопросы имитостойкости шифров.	8	4				4	
6. Шифры, не распространяющие искажений.	8	4				4	
Раздел 3. Схемы разделения секрета							
7. Пороговые схемы разделения секрета.	16	2		6	6	8	Лабораторная работа. Домашние задания
8. Схемы разделения секрета с произвольной структурой доступа.	4	2				2	
Раздел 4. Блочные шифры							
9. Симметричные блочные шифры	28	8		6	6	14	Лабораторная работа. Домашние задания
Экзамен	36						
Итого	144	36		18	18	54	

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.

Тема 3. Математическая модель шифров

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

Формальные модели шифров. Алгебраическая модель шифра. Вероятностная модель шифра. Математические модели некоторых шифров. Математическая модель шифра простой замены. Математическая модель шифра сдвига. Математическая модель шифра перестановки. Математическая модель аффинного шифра. Математическая модель шифра Хилла.

Раздел 2. Надежность шифров

Тема 4. 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 5. Вопросы имитостойкости шифров.

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


Тема 6. 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 7. 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.

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

Проверяемая схема разделения секрета Фельдмана-Шамира. Совершенная проверяемая схема разделения секрета Педерсона-Шамира. Схемы разделения секрета на основе n -разрядных равновесных двоичных кодов.

Тема 8. 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 9. 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. 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

Практические (семинарские) занятия не предусмотрены учебным планом.

7. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)

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.

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. Рацеев. Ульяновск : УлГУ, 2016. 55 с.


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.

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

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 4. Совершенные шифры

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 шифрованного файла при известном ключе.

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

Раздел 3. Схемы разделения секрета

Тема 7. 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 9. 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

Курсовые и контрольные работы не предусмотрены учебным планом дисциплины.

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ (ЗАЧЕТУ)

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

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

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

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

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	6	Экзамен, проверка лабораторных работ, проверка решения задач
2. Математические модели открытых текстов	Проработка учебного материала, подготовка к сдаче экзамена	2	Экзамен
3. Математическая модель шифров	Проработка учебного материала, подготовка к сдаче экзамена	2	Экзамен
4. Совершенные шифры.	Проработка учебного материала, лабораторные работы, подготовка к сдаче экзамена, решение задач	12	Экзамен, проверка лабораторных работ, проверка решения задач
5. Вопросы имитостойкости шифров.	Проработка учебного материала, подготовка к сдаче экзамена, решение задач	4	Экзамен, проверка решения задач
6. Шифры, не распространяющие искажений.	Проработка учебного материала, подготовка к сдаче экзамена	4	Экзамен
7. Пороговые схемы разделения секрета.	Проработка учебного материала, лабораторные работы, подготовка к сдаче экзамена, решение задач	8	Экзамен, проверка лабораторных работ, проверка решения задач
8. Схемы разделения секрета с произвольной структурой доступа.	Проработка учебного материала, подготовка к сдаче экзамена, решение задач	2	Экзамен
9. Симметричные блочные шифры	Проработка учебного материала, лабораторные работы, подготовка к сдаче экзамена	14	Экзамен, проверка лабораторных работ

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

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>

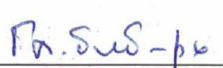
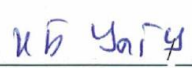

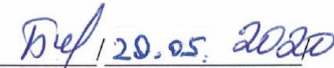
дополнительная

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://biblionline.ru/bcode/433610>
2. ОСТ-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. — URL: <https://gostexpert.ru/gost/gost-34.10-2012>
 - 2.2. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования. М.: Стандартинформ, 2013. — URL: <https://gostexpert.ru/gost/gost-34.11-2012>


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 специальности 10.05.03 «Информационная безопасность автоматизированных систем». / С. М. Рацеев; УлГУ, Фак. математики, информ. и авиац. технологий. - Ульяновск : УлГУ, 2019. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 165 КБ). - Текст : электронный. Режим доступа: <http://lib.ulsu.ru/MegaPro/Download/MObject/4674>

Согласовано:

должность сотрудника научной библиотеки ФИО подпись дата

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

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 : электронно-библиотечная система : сайт / группа компаний Ай Пи Ар Медиа. - Саратов, [2020]. – URL: <http://www.iprbookshop.ru>. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. ЮРАЙТ : электронно-библиотечная система : сайт / ООО Электронное издательство ЮРАЙТ. – Москва, [2020]. - URL: <https://www.biblio-online.ru>. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. Консультант студента : электронно-библиотечная система : сайт / ООО Политехресурс. – Москва, [2020]. – URL: http://www.studentlibrary.ru/catalogue/switch_kit/x2019-128.html. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Лань : электронно-библиотечная система : сайт / ООО ЭБС Лань. – Санкт-Петербург, [2020]. – URL: <https://e.lanbook.com>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Znanium.com : электронно-библиотечная система : сайт / ООО Знаниум. - Москва, [2020]. - URL: <http://znanium.com>. – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

1.6. Clinical Collection : коллекция для медицинских университетов, клиник, медицинских библиотек // EBSCOhost : [портал]. – URL: <http://web.a.ebscohost.com/ehost/search/advanced?vid=1&sid=e3ddfb99-a1a7-46dd-a6eb-2185f3e0876a%40sessionmgr4008>. – Режим доступа : для авториз. пользователей. – Текст : электронный.

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

3. Базы данных периодических изданий:

3.1. База данных периодических изданий : электронные журналы / ООО ИВИС. - Москва, [2020]. – URL: <https://dlib.eastview.com/browse/udb/12>. – Режим доступа : для авториз. пользователей. – Текст : электронный.

3.2. eLIBRARY.RU: научная электронная библиотека : сайт / ООО Научная Электронная Библиотека. – Москва, [2020]. – URL: <http://elibrary.ru>. – Режим доступа : для авториз. пользователей. – Текст : электронный


3.3. «Grebennikon» : электронная библиотека / ИД Гребенников. – Москва, [2020]. – URL: <https://id2.action-media.ru/Personal/Products>. – Режим доступа : для авториз. пользователей. – Текст : электронный.

4. Национальная электронная библиотека : электронная библиотека : федеральная государственная информационная система : сайт / Министерство культуры РФ ; РГБ. – Москва, [2020]. – URL: <https://нэб.рф>. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. [SMART Imagebase](https://ebsco.smartimagebase.com/?TOKEN=EBSCO-1a2ff8c55aa76d8229047223a7d6dc9c&custid=s6895741) // EBSCOhost : [портал]. – URL: <https://ebsco.smartimagebase.com/?TOKEN=EBSCO-1a2ff8c55aa76d8229047223a7d6dc9c&custid=s6895741>. – Режим доступа : для авториз. пользователей. – Изображение : электронные.

6. Федеральные информационно-образовательные порталы:

6.1. [Единое окно доступа к образовательным ресурсам](#) : федеральный портал /

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

учредитель ФГАОУ ДПО ЦРГОП и ИТ. – URL: <http://window.edu.ru/>. – Текст : электронный.

6.2. [Российское образование](http://www.edu.ru/) : федеральный портал / учредитель ФГАОУ ДПО ЦРГОП и ИТ. – URL: [http://www.edu.ru.](http://www.edu.ru/) – Текст : электронный.

7. Образовательные ресурсы УлГУ:


7.1. Электронная библиотека УлГУ : модуль АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: <http://lib.ulsu.ru/MegaPro/Web>. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.


7.2. Образовательный портал УлГУ. – URL: <http://edu.ulsu.ru>. – Режим доступа : для зарегистр. пользователей. – Текст : электронный.

Согласовано:

Зам.нач. УИТиТ
должность сотрудника УИТиТ

/ Клочкова А.В.
ФИО

 20.05.2020
подпись дата

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

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Помещение 3/317. Аудитория для проведения практических и лабораторных занятий, текущего контроля и промежуточной аттестации, групповых и индивидуальных консультаций с набором демонстрационного оборудования для обеспечения тематических иллюстраций. Помещение укомплектовано ученической доской и комплектом мебели (посадочных мест – 24). Генератор шума для акустического зашумления помещения. Сканирующий радиоприемник AP 3000 А. Широкополосная антенна. Осциллограф АСК 2102. Прибор В6-9 (селективный вольтметр). Генератор НЧ ГЗ-118. Поисковый прибор ST 032 «Пиранья». Имитатор закладных устройств ИМФ-2. Универсальный акустический излучатель к генератору акустического шума OMS-2000. Универсальный электромагнитный излучатель к генератору акустического шума. Генератор электромагнитного зашумления Гром-ЗИ4. Детектор поля D 006. Экран настенный, мультимедийный проектор. Информационные плакаты. Компьютер, Wi-Fi с доступом к сети «Интернет», ЭИОС, ЭБС. 432017, Ульяновская область, г. Ульяновск, ул. Набережная реки Свияги, д. 106 (3 корпус).

Помещение 503. Аудитория для проведения практических и лабораторных занятий, текущего контроля и промежуточной аттестации, групповых и индивидуальных консультаций. Помещение укомплектовано ученической доской и комплектом мебели (посадочных мест – 10). Компьютеры, Wi-Fi с доступом к сети «Интернет», ЭИОС, ЭБС. 432017, Ульяновская область, г. Ульяновск, р-н Железнодорожный, ул. Набережная р. Свияги, № 106 (1 корпус).

Аудитория 24б для проведения лекционных, лабораторных и практических занятий, текущего контроля и промежуточной аттестации, групповых и индивидуальных консультаций. 11 персональных компьютеров, проектор, экран, системы защиты информации: Соболев, Аккорд, Dallas Lock, Secret Net Studio. Сервер Vmark, АПКШ "Континент", Маршрутизаторы Cisco, Система защиты информации ViPNet. 432017, Ульяновская обл, г Ульяновск, ул Набережная реки Свияги, д 106-2 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.

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;

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

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

Разработчик Вашта / Рацев С.М. /
подпись ФИО

ЛИСТ ИЗМЕНЕНИЙ

№ п/п	Содержание изменения или ссылка на прилагаемый текст изменения	ФИО заведующего кафедрой, реализующей дисциплину/вы- пускающей кафедрой	Подпись	Дата
1.	Внесение изменений в п/п в) Профессиональные базы данных, информационно-справочные системы п. 11 «Учебно-методическое и информационное обеспечение дисциплины» с оформлением приложения № 1	Андреев А.С.		12.05.2021 Протокол заседания кафедры № 12
1.	Внесение изменений в п/п в) Профессиональные базы данных, информационно-справочные системы п. 11 «Учебно-методическое и информационное обеспечение дисциплины» с оформлением приложения № 2	Андреев А.С.		11.05.2022 Протокол заседания кафедры № 13
2.	Внесение изменений в п/п в) Профессиональные базы данных, информационно-справочные системы п. 11 «Учебно-методическое и информационное обеспечение дисциплины» с оформлением приложения № 3	Андреев А.С.		12.04.2023 Протокол заседания кафедры № 12

в) Профессиональные базы данных, информационно-справочные системы**1. Электронно-библиотечные системы:**

1.1. IPRbooks : электронно-библиотечная система : сайт / группа компаний Ай Пи Ар Медиа. - Саратов, [2021]. – URL: <http://www.iprbookshop.ru>. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. ЮРАЙТ : электронно-библиотечная система : сайт / ООО Электронное издательство ЮРАЙТ. – Москва, [2021]. - URL: <https://urait.ru>. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. Консультант студента : электронно-библиотечная система : сайт / ООО Политехресурс. – Москва, [2021]. – URL: <https://www.studentlibrary.ru/cgi-bin/mb4x>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Консультант врача : электронно-библиотечная система : сайт / ООО Высшая школа организации и управления здравоохранением-Комплексный медицинский консалтинг. – Москва, [2021]. – URL: <https://www.rosmedlib.ru>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО Букап. – Томск, [2021]. – URL: <https://www.books-up.ru/ru/library/> . – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.6. Лань : электронно-библиотечная система : сайт / ООО ЭБС Лань. – Санкт-Петербург, [2021]. – URL: <https://e.lanbook.com>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. **Znanium.com** : электронно-библиотечная система : сайт / ООО Знаниум. - Москва, [2021]. - URL: <http://znanium.com> . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

1.8. Clinical Collection : коллекция для медицинских университетов, клиник, медицинских библиотек // EBSCOhost : [портал]. – URL: <http://web.b.ebscohost.com/ehost/search/advanced?vid=1&sid=9f57a3e1-1191-414b-8763-e97828f9f7e1%40sessionmgr102> . – Режим доступа : для авториз. пользователей. – Текст : электронный.

1.9. Русский язык как иностранный : электронно-образовательный ресурс для иностранных студентов : сайт / ООО Компания «Ай Пи Ар Медиа». – Саратов, [2021]. – URL: <https://ros-edu.ru>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. /ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2021].

3. Базы данных периодических изданий:

3.1. База данных периодических изданий : электронные журналы / ООО ИВИС. - Москва, [2021]. – URL: <https://dlib.eastview.com/browse/udb/12>. – Режим доступа : для авториз. пользователей. – Текст : электронный.

3.2. eLIBRARY.RU: научная электронная библиотека : сайт / ООО Научная Электронная Библиотека. – Москва, [2021]. – URL: <http://elibrary.ru>. – Режим доступа : для авториз. пользователей. – Текст : электронный

3.3. «Grebennikon» : электронная библиотека / ИД Гребенников. – Москва, [2021]. – URL: <https://id2.action-media.ru/Personal/Products>. – Режим доступа : для авториз. пользователей. – Текст : электронный.

4. Национальная электронная библиотека : электронная библиотека : федеральная государственная информационная система : сайт / Министерство культуры РФ ; РГБ. – Москва, [2021]. – URL: <https://нэб.рф>. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. SMART Imagebase // EBSCOhost : [портал]. – URL: <https://ebco.smartimagebase.com/?TOKEN=EBSCO-1a2ff8c55aa76d8229047223a7d6dc9c&custid=s6895741>. – Режим доступа : для авториз. пользователей. – Изображение : электронные.

6. Федеральные информационно-образовательные порталы:

6.1. [Единое окно доступа к образовательным ресурсам](#) : федеральный портал / учредитель

ФГАОУ ДПО ЦРГОП и ИТ. – URL: <http://window.edu.ru/> . – Текст : электронный.

6.2. [Российское образование](http://www.edu.ru) : федеральный портал / учредитель ФГАОУ ДПО ЦРГОП и ИТ. – URL: <http://www.edu.ru>. – Текст : электронный.

7. Образовательные ресурсы УлГУ:

7.1. Электронная библиотека УлГУ : модуль АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: <http://lib.ulsu.ru/MegaPro/Web>. – Режим доступа : для пользователей научной библиотеки. – Текст: электронный.

Согласовано:

Зам.нач. УИТиТ
должность сотрудника УИТиТ

/ Ключкова А.В.
ФИО


подпись

04.05.2021
дата

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. Цифровой образовательный ресурс IPRsmart : электронно-библиотечная система : сайт / ООО Компания «Ай Пи Ар Медиа». - Саратов, [2022]. – URL: <http://www.iprbookshop.ru>. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. Образовательная платформа ЮРАЙТ : образовательный ресурс, электронная библиотека : сайт / ООО Электронное издательство ЮРАЙТ. – Москва, [2022]. - URL: <https://urait.ru>. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. База данных «Электронная библиотека технического ВУЗа (ЭБС «Консультант студента») : электронно-библиотечная система : сайт / ООО Политехресурс. – Москва, [2022]. – URL: <https://www.studentlibrary.ru/cgi-bin/mb4x>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Консультант врача. Электронная медицинская библиотека : база данных : сайт / ООО Высшая школа организации и управления здравоохранением-Комплексный медицинский консалтинг. – Москва, [2022]. – URL: <https://www.rosmedlib.ru>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО Букап. – Томск, [2022]. – URL: <https://www.books-up.ru/ru/library/>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.6. ЭБС Лань : электронно-библиотечная система : сайт / ООО ЭБС Лань. – Санкт-Петербург, [2022]. – URL: <https://e.lanbook.com>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. ЭБС Znanium.com : электронно-библиотечная система : сайт / ООО Знаниум. - Москва, [2022]. - URL: <http://znanium.com> . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

1.8. Clinical Collection : научно-информационная база данных EBSCO // EBSCOhost : [портал]. – URL: <http://web.b.ebscohost.com/ehost/search/advanced?vid=1&sid=9f57a3e1-1191-414b-8763-e97828f9f7e1%40sessionmgr102> . – Режим доступа : для авториз. пользователей. – Текст : электронный.

1.9. База данных «Русский как иностранный» : электронно-образовательный ресурс для иностранных студентов : сайт / ООО Компания «Ай Пи Ар Медиа». – Саратов, [2022]. – URL: <https://ros-edu.ru>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. /ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2022].

3. Базы данных периодических изданий:

3.1. База данных периодических изданий EastView : электронные журналы / ООО ИВИС. - Москва, [2022]. – URL: <https://dlib.eastview.com/browse/udb/12>. – Режим доступа : для авториз. пользователей. – Текст : электронный.

3.2. eLIBRARY.RU: научная электронная библиотека : сайт / ООО Научная Электронная Библиотека. – Москва, [2022]. – URL: <http://elibrary.ru>. – Режим доступа : для авториз. пользователей. – Текст : электронный

3.3. Электронная библиотека «Издательского дома «Гребенников» (Grebinnikon) : электронная библиотека / ООО ИД Гребенников. – Москва, [2022]. – URL: <https://id2.action-media.ru/Personal/Products>. – Режим доступа : для авториз. пользователей. – Текст : электронный.

4. Федеральная государственная информационная система «Национальная электронная библиотека» : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2022]. – URL: <https://нэб.рф>. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. [SMART Imagebase](http://www.ebsco.com) : научно-информационная база данных EBSCO // EBSCOhost

: [портал]. – URL: <https://ebSCO.smartimagebase.com/?TOKEN=EBSCO-1a2ff8c55aa76d8229047223a7d6dc9c&custid=s6895741>. – Режим доступа : для авториз. пользователей. – Изображение : электронные.

6. Федеральные информационно-образовательные порталы:

6.1. [Единое окно доступа к образовательным ресурсам](http://window.edu.ru/) : федеральный портал . – URL: <http://window.edu.ru/> . – Текст : электронный.

6.2. [Российское образование](http://www.edu.ru) : федеральный портал / учредитель ФГАУ «ФИЦТО». – URL: <http://www.edu.ru>. – Текст : электронный.

7. Образовательные ресурсы УлГУ:

7.1. Электронная библиотечная система УлГУ : модуль «Электронная библиотека» АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: <http://lib.ulsu.ru/MegaPro/Web>. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

Согласовано:

Зам.нач. УИТиТ
должность сотрудника УИТиТ

/ Ключкова А.В.
ФИО


подпись

/
дата

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. Цифровой образовательный ресурс IPRsmart : электронно-библиотечная система : сайт / ООО Компания «Ай Пи Ар Медиа». - Саратов, [2023]. – URL: <http://www.iprbookshop.ru>. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. Образовательная платформа ЮРАЙТ : образовательный ресурс, электронная библиотека : сайт / ООО Электронное издательство «ЮРАЙТ». – Москва, [2023]. - URL: <https://urait.ru>. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. База данных «Электронная библиотека технического ВУЗа (ЭБС «Консультант студента») : электронно-библиотечная система : сайт / ООО «Политехресурс». – Москва, [2023]. – URL: <https://www.studentlibrary.ru/cgi-bin/mb4x>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Консультант врача. Электронная медицинская библиотека : база данных : сайт / ООО «Высшая школа организации и управления здравоохранением-Комплексный медицинский консалтинг». – Москва, [2023]. – URL: <https://www.rosmedlib.ru>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО «Букап». – Томск, [2023]. – URL: <https://www.books-up.ru/ru/library/> . – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.6. ЭБС Лань : электронно-библиотечная система : сайт / ООО ЭБС «Лань». – Санкт-Петербург, [2023]. – URL: <https://e.lanbook.com>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. ЭБС **Znanium.com** : электронно-библиотечная система : сайт / ООО «Знаниум». - Москва, [2023]. - URL: <http://znanium.com> . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. / ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2023].

3. Базы данных периодических изданий:

3.1. eLIBRARY.RU: научная электронная библиотека : сайт / ООО «Научная Электронная Библиотека». – Москва, [2023]. – URL: <http://elibrary.ru>. – Режим доступа : для авториз. пользователей. – Текст : электронный

3.2. Электронная библиотека «Издательского дома «Гребенников» (Grebinnikon) : электронная библиотека / ООО ИД «Гребенников». – Москва, [2023]. – URL: <https://id2.action-media.ru/Personal/Products>. – Режим доступа : для авториз. пользователей. – Текст : электронный.

4. Федеральная государственная информационная система «Национальная электронная библиотека» : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2023]. – URL: <https://нэб.рф>. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. Российское образование : федеральный портал / учредитель ФГАУ «ФИЦТО». – URL: <http://www.edu.ru>. – Текст : электронный.

6. Электронная библиотечная система УлГУ : модуль «Электронная библиотека» АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: <http://lib.ulsu.ru/MegaPro/Web>. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.