


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

УТВЕРЖДЕНО

решением Учёного совета факультета математики,
информационных и авиационных технологий

от «16» июня 2020 г., протокол № 5/20

Председатель _____ / М.А. Волков
«16» июня 2020 г.



РАБОЧАЯ ПРОГРАММА

| | |
|------------|---|
| Дисциплина | Криптография |
| Факультет | Математики, информационных и авиационных технологий |
| Кафедра | Телекоммуникационных технологий и сетей |
| Курс | 3 |

Направление: 09.03.02 «Информационные системы и технологии»
код направления (специальности), полное наименование

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

Дата введения в учебный процесс УлГУ: « 1 » сентября 2020 г.

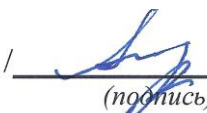
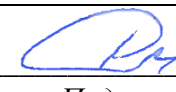
Программа актуализирована на заседании кафедры: протокол № _____ от _____ 20____ г.


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. кафедрой ИБиТУ, д.ф-м.н, профессор |

| СОГЛАСОВАНО | СОГЛАСОВАНО |
|---|---|
| Заведующий кафедрой информационной безопасности и теории управления, реализующей дисциплину | Заведующий выпускающей кафедрой телекоммуникационных технологий и сетей |
|  / _____ / Андреев А.С. / (подпись) (Ф.И.О.) |  / _____ / Смагин А.А. / Подпись ФИО «16» июня 2020 г. |
| «16» 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 дисциплинам по выбору блока Б1.В.ДВ образовательной программы и читается в 6-м семестре студентам по направлению подготовки «Информационные системы и технологии» очной формы обучения и в 4-м семестре студентам по направлению подготовки «Информационные системы и технологии» заочной формы обучения.

Для успешного освоения дисциплины необходимы знания основных фактов из базовых курсов: «Математический анализ», «Алгебра», «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: «Инфокоммуникационные системы и сети», 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-6 Способен разрабатывать алгоритмы и программы, пригодные для практического применения в области информационных систем и технологий | Знать: 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 кольцах и полях с подстановками, многочленами, матрицами, в том числе с использованием компьютерных программ; Владеть: |

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

| | |
|---|--|
| | навыками эффективного вычисления в кольцах вычетов и в кольцах многочленов. |
| ОПК-7 Способен осуществлять выбор платформ и инструментальных программноаппаратных средств для реализации информационных систем | Знать: основные виды симметричных и асимметричных криптографических алгоритмов; математические модели шифров; Владеть: криптографической терминологией; |
| ПК-3 Способен использовать математические методы обработки, анализа и синтеза результатов исследований | Знать: основные виды симметричных и асимметричных криптографических алгоритмов; математические модели шифров; Уметь: корректно применять симметричные и асимметричные криптографические алгоритмы; Владеть: криптографической терминологией; |


4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего) 2.

4.2. Объем дисциплины по видам учебной работы:

Форма обучения очная


| Вид учебной работы | Количество часов (форма обучения - дневная) | | | |
|---|---|--|--|--|
| | Всего по плану | В т.ч. по семестрам | | |
| | | 6 | | |
| Контактная работа обучающихся с преподавателем | 36 | 36 | | |
| Аудиторные занятия: | | | | |
| • Лекции | 18 | 18 | | |
| • Практические и семинарские занятия | 18 | 18 | | |
| • Лабораторные работы (лабораторный практикум) | | | | |
| Самостоятельная работа | 36 | 36 | | |
| Форма текущего контроля знаний и контроля самостоятельной | | проверка решения задач, контрольные работы | | |

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

| | | | | |
|--|----|-------|--|--|
| работы | | | | |
| Курсовая работа | | | | |
| Экзамен | | | | |
| Всего часов по дисциплине | 72 | 72 | | |
| Виды промежуточной аттестации (экзамен, зачет) | | зачет | | |
| Общая трудоемкость в зач. ед. | 2 | 2 | | |

Форма обучение заочная


| Вид учебной работы | Количество часов (форма обучения - дневная) | | | |
|--|---|--|--|--|
| | Всего по плану | В т.ч. по семестрам | | |
| | | 6 | | |
| Контактная работа обучающихся с преподавателем | 16 | 16 | | |
| Аудиторные занятия: | | | | |
| • Лекции | 10 | 10 | | |
| • Практические и семинарские занятия | 6 | 6 | | |
| • Лабораторные работы (лабораторный практикум) | | | | |
| Самостоятельная работа | 52 | 52 | | |
| Форма текущего контроля знаний и контроля самостоятельной работы | | проверка решения задач, контрольные работы | | |
| Курсовая работа | | | | |
| Контроль | 4 | 4 | | |
| Всего часов по дисциплине | 72 | 72 | | |
| Виды промежуточной аттестации (экзамен, зачет) | | зачет | | |

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

| | | | | |
|-------------------------------|---|---|--|--|
| Общая трудоемкость в зач. ед. | 2 | 2 | | |
|-------------------------------|---|---|--|--|

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 | 8 | 2 | 2 | | 2 | 4 | проверка решения задач |
| 2. Математические модели открытых текстов и шифров | 8 | 2 | 2 | | | 4 | |
| Раздел 2. Надежность шифров | | | | | | | |
| 3. Совершенные шифры. | 8 | 2 | 2 | | 2 | 4 | проверка решения задач |
| 4. Вопросы имитостойкости шифров. | 8 | 2 | 2 | | | 4 | |
| 5. Шифры, не распространяющие искажений. | 8 | 2 | 2 | | | 4 | |
| Раздел 3. Схемы разделения секрета | | | | | | | |
| 6. Пороговые схемы разделения секрета. | 8 | 2 | 2 | | 2 | 4 | проверка решения задач |
| 7. Схемы разделения секрета с произвольной структурой доступа. | 8 | 2 | 2 | | | 4 | контрольная работа |
| Раздел 4. Блочные шифры | | | | | | | |
| 8. Симметричные блочные шифры | 8 | 2 | 2 | | 3 | 4 | проверка решения задач |
| 9. Асимметричные шифры | 8 | 2 | 2 | | | 4 | |
| | | | | | | | |
| | | | | | | | |
| Итого | 72 | 18 | 18 | | 9 | 36 | |

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

Форма обучения _____ заочная _____


| 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 | 6 | 1 | 1 | | | 4 | Домашние задания |
| 2. Математические модели открытых текстов и шифров | 3 | 1 | | | | 2 | |
| Раздел 2. Надежность шифров | | | | | | | |
| 3. Совершенные шифры. | 6 | 1 | 1 | | | 4 | Домашние задания |
| 4. Вопросы имитостойкости шифров. | 5 | 1 | | | | 4 | |
| 5. Шифры, не распространяющие искажений. | 5 | 1 | | | | 4 | |
| Раздел 3. Схемы разделения секрета | | | | | | | |
| 6. Пороговые схемы разделения секрета. | 10 | 1 | 1 | | | 8 | Домашние задания |
| 7. Схемы разделения секрета с произвольной структурой доступа. | 8 | 1 | 1 | | | 6 | Контрольная работа |
| Раздел 4. Блочные шифры | | | | | | | |
| 8. Симметричные блочные шифры | 12 | 1 | 1 | | 1 | 10 | Домашние задания |
| 9. Асимметричные шифры | 13 | 2 | 1 | | 1 | 10 | Домашние задания |
| Контроль | 4 | | | | | | |
| Итого | 72 | 10 | 6 | | | 52 | |

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

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

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 и шифров

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 запретных m -грамм. 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 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. 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.

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


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

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. 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.

Тема 9. Асимметричные шифры.

Система Диффи-Хеллмана. Способы выбора образующего элемента. Модификация системы Диффи-Хеллмана на эллиптических кривых. Криптосистема без передачи ключа (шифр Шамира). Описание системы. Надежность системы. Модификация системы на эллиптических кривых. Шифр Эль-Гамала. Ограничения на параметры системы. Модификация шифра Эль-Гамала на эллиптических кривых. Шифр RSA. Понятие односторонней функции с «лазейкой». Описание шифра RSA. Электронная подпись. Общие положения. Задачи, решаемые с помощью электронных подписей. Надежность электронной подписи. Электронная подпись на основе шифрсистем с открытыми ключами. Электронные подписи на основе симметричных криптосистем. Примеры электронных подписей. Подпись Фиата-Шамира. Подпись Эль-Гамала. Подпись RSA. Подпись Шнорра. Одноразовые электронные подписи.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

Некоторые семинарские занятия 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

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 и шифров

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. 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.

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. Режим электронной

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

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

Тема 9. Асимметричные шифры.

Система Диффи-Хеллмана. Способы выбора образующего элемента. Модификация системы Диффи-Хеллмана на эллиптических кривых. Криптосистема без передачи ключа (шифр Шамира). Описание системы. Надежность системы. Модификация системы на эллиптических кривых. Шифр Эль-Гамала. Ограничения на параметры системы. Модификация шифра Эль-Гамала на эллиптических кривых. Шифр RSA. Понятие односторонней функции с «лазейкой». Описание шифра RSA. Электронная подпись. Общие положения. Задачи, решаемые с помощью электронных подписей. Надежность электронной подписи. Электронная подпись на основе шифрсистем с открытыми ключами. Электронные подписи на основе симметричных криптосистем. Примеры электронных подписей. Подпись Фиата-Шамира. Подпись Эль-Гамала. Подпись RSA. Подпись Шнора. Одноразовые электронные подписи.

7. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)

Не предусмотрено учебным планом

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.
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

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

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

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.

Криптография с открытым ключом


40. Алгоритм быстрого возведения в степень. Задачи, приводящие к криптографии с открытым ключом и их решение.

41. Схема Диффи-Хеллмана.

42. Криптосистема без передачи ключа (шифр Шамира).

43. Вероятностный шифр Эль-Гамала.

44. Шифр RSA.

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

45. Рюкзачные криптосистемы.
46. Методы взлома шифров, основанных на дискретном логарифмировании: Полный перебор, метод «Шаг младенца, шаг великана».
47. Методы взлома шифров, основанных на дискретном логарифмировании: Метод исчисления порядка.

Хеш-функции

48. Хеш-функции. Требования, предъявляемые к хеш-функциям.
49. Криптографические хеш-функции. Способы построения криптографических хеш-функций.


Электронные подписи

50. Электронная подпись RSA.
51. Электронные деньги на основе RSA.
52. Электронная подпись Фиата-Шамира.
53. Электронная подпись Эль-Гамала.
54. Электронная подпись Шнорра.
55. Электронная подпись с доверенным посредником на основе симметричной криптосистемы.

10. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

Форма обучения очная


| 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 | 4 | Зачет, проверка лабораторных работ, проверка решения задач |
| 2. Математические модели открытых текстов и шифров | Проработка учебного материала, подготовка к сдаче экзамена | 4 | Зачет |
| 3. Совершенные шифры. | Проработка учебного материала, лабораторные работы, подготовка к сдаче экзамена, решение задач | 4 | Зачет, 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 |
| 6. Пороговые схемы разделения секрета. | Проработка учебного материала, лабораторные работы, подготовка к сдаче экзамена, решение задач | 4 | Зачет, проверка решения задач |
| 7. Схемы разделения секрета с произвольной структурой доступа. | Проработка учебного материала, подготовка к сдаче экзамена, решение задач | 4 | Зачет |
| 8. Симметричные блочные шифры | Проработка учебного материала, лабораторные работы, подготовка к сдаче экзамена | 4 | Зачет, проверка решения задач |
| 9. Асимметричные | Проработка учебного материала, | 4 | Зачет |

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

| | | | |
|-------|-----------------------------|--|--|
| шифры | подготовка к сдаче экзамена | | |
|-------|-----------------------------|--|--|

Форма обучения заочная

| 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 | 4 | Зачет, проверка лабораторных работ, проверка решения задач |
| 2. Математические модели открытых текстов | Проработка учебного материала, подготовка к сдаче экзамена | 2 | Зачет |
| 3. Совершенные шифры. | Проработка учебного материала, лабораторные работы, подготовка к сдаче экзамена, решение задач | 4 | Зачет, 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 |
| 6. Пороговые схемы разделения секрета. | Проработка учебного материала, лабораторные работы, подготовка к сдаче экзамена, решение задач | 8 | Зачет, проверка решения задач |
| 7. Схемы разделения секрета с произвольной структурой доступа. | Проработка учебного материала, подготовка к сдаче экзамена, решение задач | 6 | Зачет |
| 8. Симметричные блочные шифры | Проработка учебного материала, лабораторные работы, подготовка к сдаче экзамена | 10 | Зачет, проверка решения задач |
| 9. Асимметричные шифры | Проработка учебного материала, подготовка к сдаче экзамена | 10 | Зачет |

| | | |
|--|-------|---|
| 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>

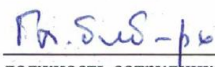

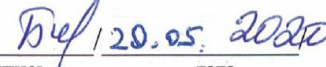
Дополнительная

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://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. — 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 «Криптография» для студентов направления подготовки 09.03.02 «Информационные системы и технологии» / С. М. Рацеев; УлГУ, Фак. математики, информ. и авиац. технологий. - Ульяновск : УлГУ, 2019. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 167 КБ). - Текст : электронный. Режим доступа: <http://lib.ulsu.ru/MegaPro/Download/MObject/4676>

Согласовано:




 должность сотрудника научной библиотеки ФИО подпись дата

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

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

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 // 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 / 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.

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

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

Согласовано:

Зам.нач. УИТиГ / Клочкова А.В. 20.05.2020
 должность сотрудника УИТиГ ФИО 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.

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.

Разработчик  / Андреев А.С. /
 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. 4.2 Объем дисциплины по видам учебной работы п. «Общая трудоемкость дисциплины» с оформлением приложения 1 | Андреев А.С. |  | 08.04.2020 Протокол заседания кафедры № 12 |
| 2 | Внесение изменений в п. 13 «Специальные условия для обучающихся с ограниченными возможностями здоровья» с оформлением приложения 2 | Андреев А.С. |  | 08.04.2020 Протокол заседания кафедры № 12 |
| 3 | Внесение изменений в п/п а) Список рекомендуемой литературы п. 11 «Учебно-методическое и информационное обеспечение дисциплины» с оформлением приложения 3 | Андреев А.С. |  | 27.05.2020 Протокол заседания кафедры № 14 |
| 4 | Внесение изменений в п/п в) Профессиональные базы данных, информационно-справочные системы п. 11 «Учебно-методическое и информационное обеспечение дисциплины» с оформлением приложения 4 | Андреев А.С. |  | 27.05.2020 Протокол заседания кафедры № 14 |

| | | |
|--|-------|---|
| Министерство науки и высшего образования РФ Ульяновский государственный университет | Форма |  |
| Ф-Рабочая программа дисциплины | | |


Приложение 1

4.2. Объем дисциплины по видам учебной работы:


| Вид учебной работы | Количество часов (форма обучения - очная) | | | |
|--|---|--|--|--|
| | Всего по плану | В т.ч. по семестрам | | |
| | | 6 | | |
| Контактная работа обучающихся с преподавателем | 36 | 36/36* | | |
| Аудиторные занятия: | | | | |
| • Лекции | 18 | 18/18* | | |
| • Практические и семинарские занятия | 18 | 18/18* | | |
| • Лабораторные работы (лабораторный практикум) | | | | |
| Самостоятельная работа | 36 | 36 | | |
| Форма текущего контроля знаний и контроля самостоятельной работы | | проверка решения задач, контрольные работы | | |
| Курсовая работа | | | | |
| Экзамен | | | | |
| Всего часов по дисциплине | 72 | 72 | | |
| Виды промежуточной аттестации (экзамен, зачет) | | зачет | | |
| Общая трудоемкость в зач. ед. | 2 | 2 | | |

*Количество часов работы ППС с обучающимися в дистанционном формате с применением электронного обучения

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 РФ Ульяновский государственный университет | Форма |  |
| Ф-Рабочая программа дисциплины | | |

| Вид учебной работы | Количество часов (форма обучения - заочная) | | | |
|--|---|--|--|--|
| | Всего по плану | В т.ч. по семестрам | | |
| | | 6 | | |
| Контактная работа обучающихся с преподавателем | 16 | 16/16* | | |
| Аудиторные занятия: | | | | |
| • Лекции | 10 | 10/10* | | |
| • Практические и семинарские занятия | 6 | 6/6* | | |
| • Лабораторные работы (лабораторный практикум) | | | | |
| Самостоятельная работа | 52 | 52 | | |
| Форма текущего контроля знаний и контроля самостоятельной работы | | проверка решения задач, контрольные работы | | |
| Курсовая работа | | | | |
| Контроль | 4 | 4 | | |
| Всего часов по дисциплине | 72 | 72 | | |
| Виды промежуточной аттестации (экзамен, зачет) | | зачет | | |
| Общая трудоемкость в зач. ед. | 2 | 2 | | |

| | | |
|--|-------|---|
| Министерство науки и высшего образования РФ Ульяновский государственный университет | Форма |  |
| Ф-Рабочая программа дисциплины | | |

Приложение 2

13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ


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

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации;

- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации;

- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

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

| | | |
|--|-------|---|
| Министерство науки и высшего образования РФ Ульяновский государственный университет | Форма |  |
| Ф-Рабочая программа дисциплины | | |

Приложение 3

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. 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. — 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 «Криптография» для студентов направления подготовки 09.03.02 «Информационные системы и технологии» / С. М. Рацеев; УлГУ, Фак. математики, информ. и авиац. технологий. - Ульяновск : УлГУ, 2019. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 167 КБ). - Текст : электронный. Режим доступа: <http://lib.ulsu.ru/MegaPro/Download/MObject/4676>

Согласовано:

П.С.С. - р.к КБ УлГУ Полина И.Р 20.05.2020
 должность сотрудника научной библиотеки ФИО подпись дата

| | | |
|--|-------|---|
| Министерство науки и высшего образования РФ Ульяновский государственный университет | Форма |  |
| Ф-Рабочая программа дисциплины | | |

Приложение 4

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

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

6. Федеральные информационно-образовательные порталы:

| | | |
|--|-------|---|
| Министерство науки и высшего образования РФ Ульяновский государственный университет | Форма |  |
| Ф-Рабочая программа дисциплины | | |

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](#) : 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.

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