


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



**УТВЕРЖДЕНО**

решением Ученого совета факультета математики, информационных и авиационных технологий  
от « 18 » 05 2021 г., протокол № 4/21

Председатель М.А. Волков  
(подпись, расшифровка подписи)  
« 18 » 05 2021 г.

### РАБОЧАЯ ПРОГРАММА

|            |   |
|------------|---|
| Дисциплина | Методы и средства криптографической защиты информации |
| Факультет  | Математики, информационных и авиационных технологий   |
| Кафедра    | Информационной безопасности и теории управления       |
| Курс       | 4   |

Специальность: 10.05.01 «Компьютерная безопасность»  
*код направления (специальности), полное наименование*

Специализация: «Математические методы защиты информации»  
*полное наименование*

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

Дата введения в учебный процесс УлГУ: « 01 » 09 2021 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 |
|--------------------------|---------|-----------------------------------|
| Рацеев Сергей Михайлович | ИБиТУ   | профессор, д.ф-м.н, доцент        |

| СОГЛАСОВАНО  | СОГЛАСОВАНО   |
|--|---|
| Заведующий кафедрой<br>«Информационная безопасность и<br>теория управления»,<br>реализующей дисциплину                     | Заведующий выпускающей кафедрой<br>«Информационная безопасность и теория<br>управления»                                     |
|  / Андреев А.С. /<br>(подпись) (Ф.И.О.) |  / Андреев А.С. /<br>(подпись) (Ф.И.О.) |
| « 12 » 05 2021 г.  | « 12 » 05 2021 г.   |

|  |       |   |
|--|-------|---|
| Министерство науки и высшего образования Российской Федерации<br>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 обязательной части цикла Б1 образовательной программы и читается в 7-м и 8-м семестрах студентам специальности «Компьютерная безопасность» очной формы обучения.

Для успешного освоения дисциплины необходимы знания основных фактов из базовых курсов: «Математический анализ», «Алгебра», «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», «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), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины «Методы и средства криптографической 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-3 – Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности | <p>Знать:</p> <p>алгоритмы проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в конечных циклических группах;</p> <p>Уметь:</p> <p>проводить вычисления в числовых и конечных кольцах и полях с подстановками, многочленами, матрицами, в том числе с использованием компьютерных программ;</p> <p>Владеть:</p> <p>навыками эффективного вычисления в кольцах выче-</p> |

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


|   |  |
|---|--|
|   | тов и в кольцах многочленов.   |
| ОПК-10 – Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности | <p>Знать:</p> <p>основные задачи, решаемые криптографическими методами;</p> <p>математические модели шифров, подходы к оценке их стойкости;</p> <p>зарубежные и российские криптографические стандарты;</p> <p>основные виды симметричных и асимметричных криптографических алгоритмов;</p> <p>Уметь:</p> <p>корректно использовать криптографические алгоритмы на практике при решении задач криптографическими методами;</p> <p>применять математические методы при исследовании криптографических алгоритмов;</p> <p>Владеть:</p> <p>криптографической терминологией;</p> <p>навыками использования типовых криптографических алгоритмов;</p> |

#### 4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

##### 4.1. Объем дисциплины в зачетных единицах (всего) 6.

##### 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                             | 8                             |  |
| Контактная работа обучающихся с преподавателем | 90/90*                                      | 54/54*                        | 36/36*                        |  |
| Аудиторные занятия:                            |   |                               |                               |  |
| • Лекции                                       | 54/54*                                      | 36/36*                        | 18/18*                        |  |
| • Практические и семинарские занятия           |   |                               |                               |  |
| • Лабораторные работы (лабораторный практикум) | 36/36*                                      | 18/18*                        | 18/18*                        |  |
| Самостоятельная работа                         | 90  | 54                            | 36                            |  |
| Форма текущего контроля знаний и контроля      |   | Лабораторные работы, проверка | Лабораторные работы, проверка |  |


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

|  |     |               |               |  |
|--|-----|---------------|---------------|--|
| самостоятельной работы                         |     | решения задач | решения задач |  |
| Курсовая работа                                | +   |               | +             |  |
| Экзамен  | 36  |               | 36            |  |
| Всего часов по дисциплине                      | 216 | 108           | 108           |  |
| Виды промежуточной аттестации (экзамен, зачет) |     | зачет         | экзамен       |  |
| Общая трудоемкость в зач. ед.                  | 6   | 3             | 3             |  |

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

**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                      |  |
| <b>Раздел 1. Математическая модель шифров</b> |       |                      |                                |                                 |                               |                        |  |
| 1. Шифры замены и перестановки                | 12    | 4                    |                                | 2                               | 2                             | 6                      | Лабораторная работа.<br>Домашние задания |
| 2. Математические модели открытых текстов     | 4     | 2                    |                                |                                 |                               | 2                      |  |
| 3. Математическая модель шифров               | 4     | 2                    |                                |                                 |                               | 2                      |  |
| <b>Раздел 2. Надежность шифров</b>            |       |                      |                                |                                 |                               |                        |  |
| 4. Совершенные шифры.                         | 24    | 8                    |                                | 4                               | 4                             | 12                     | Лабораторная работа.<br>Домашние задания |
| 5. Вопросы имитостойкости шифров.             | 8     | 4                    |                                |                                 |                               | 4                      |  |
| 6. Шифры, не распространяющие                 | 8     | 4                    |                                |                                 |                               | 4                      |  |

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

|  |     |    |  |    |    |    |  |
|--|-----|----|--|----|----|----|--|
| искажений.   |     |    |  |    |    |    |  |
| <b>Раздел 3. Схемы разделения секрета</b>                      |     |    |  |    |    |    |  |
| 7. Пороговые схемы разделения секрета.                         | 12  | 2  |  | 4  | 4  | 6  | Лабораторная работа.<br>Домашние задания |
| 8. Схемы разделения секрета с произвольной структурой доступа. | 4   | 2  |  |    |    | 2  |  |
| <b>Раздел 4. Блочные шифры</b>                                 |     |    |  |    |    |    |  |
| 9. Симметричные блочные шифры                                  | 32  | 8  |  | 8  | 8  | 16 | Лабораторная работа.<br>Домашние задания |
| 10. Шифрование с открытым ключом (8 сем)                       | 40  | 8  |  | 12 | 8  | 20 | Лабораторная работа.<br>Домашние задания |
| <b>Раздел 5. Электронные подписи</b>                           |     |    |  |    |    |    |  |
| 11. Криптографические хеш-функции                              | 8   | 4  |  |    |    | 4  |  |
| 12. Электронная подпись  | 24  | 6  |  | 6  | 4  | 12 | Лабораторная работа.<br>Домашние задания |
| Экзамен  | 36  |    |  |    |    |    |  |
| Итого  | 216 | 54 |  | 36 | 30 | 90 |  |

## 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.

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

### Тема 3. Математическая модель шифров

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<br>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. 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. Примеры итеративных блочных шифров. Шифры “Магма” и “Кузнечик” из ГОСТ Р 34.12-2015. Шифр AES.

### **Тема 10. Шифрование с открытым ключом**

Задачи, приводящие к криптографии с открытым ключом. Понятие односторонней функции. Быстрое (бинарное) возведение в степень. 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. Ограничения на параметры системы. Рюкзачные системы. Описание «проблемы рюкзака». Система Меркла-Хеллмана на основе супервозрастающей последовательности. Криптосистема Шора-Ривеста на основе конечных полей.

## **Раздел 5. Электронные подписи**

### **Тема 11. Криптографические хеш-функции**


Определение хеш-функции. Примеры хеш-функций. Целесообразность использования хеш-функций. Основные требования, которым должна удовлетворять хеш-функция. Зависимость данных требований друг от друга. Парадокс дней рождений. Построение хеш-функций. Примеры криптографических хеш-функций. Коды аутентификации. Основные понятия. Имитация и подмена для кода аутентификации. Нижние границы вероятностей имитации и подмены. Критерий достижимости нижних оценок. Оптимальные коды аутентификации. Ортогональные таблицы. Математическая модель кода аутентификации с неограниченным ключом. Примеры оптимальных кодов аутентификации с неограниченным ключом.

### **Тема 12. 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.

## **6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ**

Практические (семинарские) занятия не предусмотрены учебным планом.

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

## 7. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)

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

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

### Раздел 1. Математическая модель шифров

#### Тема 1. Шифры замены и перестановки

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

Задание.

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

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

### Раздел 3. Схемы разделения секрета



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

## 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.

### Тема 10. Шифрование с открытым ключом

Цель работы: освоить обмен ключами по схеме Диффи-Хеллмана, изучая проблему первообразных корней.

Задание. Реализовать программу, генерирующую алгоритм обмена ключей по схеме Диффи-Хеллмана.

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

### Тема 10. Шифрование с открытым ключом

Цель работы: освоить методику работы ассиметричных алгоритмов шифрования, где существует два ключа – один для шифрования, другой для расшифрования.

Задание. Требуется реализовать программу, работающую по алгоритму Эль-Гамала. Программа должна уметь работать с текстом произвольной длины.

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

## Раздел 5. Электронные подписи

### Тема 12. Электронная подпись

Цель работы: освоить методику работы электронных подписей.


Задание. Требуется реализовать электронную подпись Эль-Гамала.

Методические указания: основное внимание должно быть уделено освоению алгоритмов электронных подписей.

## 8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

*Перечень направлений исследования для курсовых работ*

1. Модели и методы распознавания открытых текстов.
2. Криптоанализ шифров с помощью генетических алгоритмов.
3. Совершенные имитостойкие шифры.
4. Шифры, близкие к экстремальным.
5. Итеративные блочные шифры.
6. Шифры, не распространяющие искажений.

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

7. Контроль целостности данных с помощью хеш-функций.
8. Оптимальные коды аутентификации.
9. Схемы разделения секрета.
10. Криптосистемы на эллиптических кривых.
11. Генераторы псевдослучайных и случайных последовательностей.
12. Шифрование изображений и видео.

Требования к оформлению курсовых работ приведено в работе: Андреев А.С., Иванцов А.М., Рацеев С.М. Методические указания по написанию курсовых и дипломных работ для студентов специальности «Компьютерная безопасность». Ульяновск: УлГУ. 2017. 40 с.

## 9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ (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.
11. Математическая модель некоторых шифров: шифр замены с конечным ключом, шифр Виженера, шифр перестановки.

### Надежность шифров

12. Определение совершенного по Шеннону шифра. Эквивалентные условия. Необходимые условия совершенного по Шеннону шифра.
13. Достаточное условие совершенного по Шеннону шифра. Теорема Шеннона.
14. Критерий совершенных шифров в классе шифров с равномерным распределением вероятностей на множестве ключей.
15. 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.
16. Примеры совершенных шифров с условиями  $|X|=|Y|=|K|$ ,  $|X|<|Y|=|K|$ ,  $|X|=|Y|<|K|$ ,  $|X|<|Y|<|K|$ .
17.  $(k|y)$ -совершенные шифры: определение, эквивалентные условия.
18. Необходимые и достаточные условия  $(k|y)$ -совершенных шифров.
19. Необходимые и достаточные условия одновременно совершенных и  $(k|y)$ -совершенных шифров.

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

20. Примеры  $(k|y)$ -совершенных шифров с условиями  $|X|=|Y|>|K|$ ,  $|X|=|Y|=|K|$ ,  $|X|=|Y|<|K|$ .  
 21. Примеры одновременно совершенного и  $(k|y)$ -совершенного шифра с условиями  $|X|=|Y|=|K|$ ,  $|X|=|Y|<|K|$ .

#### **Математическая модель шифра замены с ограниченным и неограниченным ключом**

22. Понятие опорного шифра, степени опорного шифра. Случайный и детерминированный генераторы ключевого потока. Примеры генераторов.  
 23. Определение шифра замены с ограниченным и неограниченным ключом.  
 24. Определение совершенного шифра замены, эквивалентные условия. Несовершенство в общем случае шифра замены с ограниченным ключом.  
 25. Достаточные условия совершенного шифра замены с неограниченным ключом.  
 26. Критерий совершенности шифра замены с неограниченным ключом в классе эндоморфных шифров.  
 27. Критерий совершенности шифра замены с неограниченным ключом в классе шифров с равномерным распределением на множестве ключей.

#### **Имитостойкие шифры**

28. 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.  
 29. 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.  
 30. Совершенные имитостойкие шифры замены с неограниченным ключом.

#### **Шифры, не распространяющие искажений**


31. Шифры, не распространяющие искажений типа замены знаков: определение, эквивалентные условия.  
 32. Понятие изометрии. Свойства изометрий.  
 33. Теорема А.А.Маркова. Примеры шифров, не распространяющих искажения типа замены знаков.  
 34. Шифры, не распространяющие искажений типа пропуска знаков: основные понятия.  
 35. Критерий для шифров, не распространяющих искажений типа пропуска знаков, в классе эндоморфных шифров.  
 36. Шифры, не распространяющие искажений типа вставки знаков

#### **Схемы разделения секрета**

37. Понятие  $(n,t)$  пороговой схемы разделения секрета. Пример  $(n,n)$  пороговой схемы. Схема разделения секрета на основе решения СЛАУ.  
 38. Схема разделения секрета Шамира.  
 39. Проверяемая схема разделения секрета Фельдмана-Шамира.  
 40. Совершенная проверяемая схема разделения секрета Педерсона-Шамира.  
 41. Схемы разделения секрета на основе  $n$ -разрядных равновесных двоичных кодов.  
 42. Схема разделения секрета на основе китайской теоремы об остатках.  
 43. Схемы разделения секрета для произвольных структур доступа: основные понятия. Схема Бенало-Лейхтера.  
 44. Схема Ито-Саито-Нишизеки.

#### **Симметричные блочные шифры**

45. Итеративные блочные шифры. Обратимость итеративного блочного шифра.  
 46. Шифры Фейстеля и их обратимость.  
 47. Построение раундовой функции. Входное и выходное отображения.  
 48. Слабые ключи итеративного блочного шифра.  
 49. Режимы использования симметричных блочных шифров.

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

50. Шифр Магма из ГОСТ Р 34.12-2015.

### Криптография с открытым ключом

51. Алгоритм быстрого возведения в степень. Задачи, приводящие к криптографии с открытым ключом и их решение.
52. Схема Диффи-Хеллмана.
53. Криптосистема без передачи ключа (шифр Шамира).
54. Вероятностный шифр Эль-Гамала.
55. Шифр RSA.
56. Рюкзачные криптосистемы.
57. Методы взлома шифров, основанных на дискретном логарифмировании: Полный перебор, метод «Шаг младенца, шаг великана».
58. Методы взлома шифров, основанных на дискретном логарифмировании: Метод исчисления порядка.

### Хеш-функции

59. Хеш-функции. Требования, предъявляемые к хеш-функциям.
60. Криптографические хеш-функции. Способы построения криптографических хеш-функций.

### Коды аутентификации


61. Понятие имитации и подмены кода аутентификации. Определение вероятностей  $P_{им}$ ,  $P_{подм}$ .
62. Нижние оценки для вероятности имитации и подмены кода аутентификации. Критерий достижимости нижних оценок.
63. Оптимальные коды аутентификации. Достаточные условия оптимального кода аутентификации.

### Электронные подписи


64. Электронная подпись RSA.
65. Электронные деньги на основе RSA.
66. Электронная подпись Фиата-Шамира.
67. Электронная подпись Эль-Гамала.
68. Электронная подпись Шнорра.
69. Электронная подпись с доверенным посредником на основе симметричной криптосистемы.

## 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 зачета и экзамена, решение задач | 6             | Зачет, экзамен, проверка лабораторных работ, проверка решения задач |
| 2. Математические модели открытых текстов | Проработка учебного материала, подготовка к сдаче зачета и экзамена                                     | 2             | Зачет, экзамен  |
| 3. Математическая модель шифров           | Проработка учебного материала, подготовка к сдаче зачета и экзамена                                     | 2             | Зачет, экзамен  |
| 4. Совершенные шифры.                     | Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета и экзамена, решение       | 12            | Зачет, экзамен, проверка лабораторных работ,                        |

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

|  | задач   |    | проверка решения задач  |
|--|---|----|---|
| 5. Вопросы имитостойкости шифров.                              | Проработка учебного материала, подготовка к сдаче зачета и экзамена, решение задач                      | 4  | Зачет, экзамен, проверка решения задач                              |
| 6. Шифры, не распространяющие искажений.                       | Проработка учебного материала, подготовка к сдаче зачета и экзамена                                     | 4  | Зачет, экзамен  |
| 7. Пороговые схемы разделения секрета.                         | Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета и экзамена, решение задач | 6  | Зачет, экзамен, проверка лабораторных работ, проверка решения задач |
| 8. Схемы разделения секрета с произвольной структурой доступа. | Проработка учебного материала, подготовка к сдаче зачета и экзамена, решение задач                      | 2  | Зачет, экзамен  |
| 9. Симметричные блочные шифры                                  | Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета и экзамена                | 16 | Зачет, экзамен, проверка лабораторных работ                         |
| 10. Шифрование с открытым ключом                               | Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета и экзамена, решение задач | 20 | Зачет, экзамен, проверка лабораторных работ, проверка решения задач |
| 11. Криптографические хеш-функции                              | Проработка учебного материала, подготовка к сдаче зачета и экзамена                                     | 4  | Зачет, экзамен  |
| 12. Электронная подпись  | Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета и экзамена, решение задач | 12 | Зачет, экзамен, проверка лабораторных работ, проверка решения задач |

|  |       |   |
|--|-------|---|
| Министерство науки и высшего образования Российской Федерации<br>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 «Методы и средства криптографической защиты информации» для студентов специальностей 10.05.01 «Компьютерная безопасность» и 10.05.03 «Информационная безопасность автоматизированных систем» / С. М. Рацеев; УлГУ, ФМИАТ. - Ульяновск : УлГУ, 2020. - 11 с. - Неопубликованный ресурс. - URL: <http://lib.ulsu.ru/MegaPro/Download/MObject/10712>. - Режим доступа: ЭБС УлГУ. - Текст : электронный.

Согласовано:

Р.С.С.-рь      И.Б. УлГУ      Помина И.Ю      Вел, 04.05.2021  
 должность сотрудника научной библиотеки      ФИО      подпись      дата



|  |       |   |
|--|-------|---|
| Министерство науки и высшего образования Российской Федерации<br>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, [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://gos-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.

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

**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://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.


Согласовано:

Зам.нач. УИТиТ  
должность сотрудника УИТиТ

/ Клочкова А.В.  
ФИО

  
подпись

04.05.2021  
дата

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

## 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

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 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 Vimark, 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;

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

Разработчик

подпись

ФИО