

# ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:  
Руководитель специальности



А. Н. Соколов

## РАБОЧАЯ ПРОГРАММА

дисциплины 1.О.32 Методы и средства криптографической защиты информации для специальности 10.05.03 Информационная безопасность автоматизированных систем

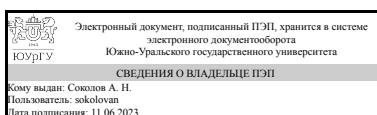
уровень Специалитет

форма обучения очная

кафедра-разработчик Защита информации

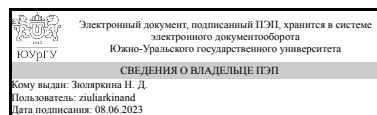
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утверждённым приказом Минобрнауки от 26.11.2020 № 1457

Зав.кафедрой разработчика,  
к.техн.н., доц.



А. Н. Соколов

Разработчик программы,  
д.физ.-мат.н., доц., профессор



Н. Д. Зюляркина

## 1. Цели и задачи дисциплины

Целью изучения дисциплины является формирование у студентов общих представлений о содержании криптографических методов защиты информации и о подходах к оценке эффективности таких методов. Задачи дисциплины: дать представление об информационной безопасности, как сфере профессиональной деятельности; раскрыть особенности криптографических методов защиты информации и содержание базовых понятий криптографии; ознакомить с основными видами шифров; ознакомить с современными стандартами криптографической защиты; дать представление об атаках на криптографические системы.

## Краткое содержание дисциплины

В рамках данной дисциплины исследуются основные типы шифров, проводится анализ их криптостойкости, изучаются основные типы атак и методы противодействия им.

## 2. Компетенции обучающегося, формируемые в результате освоения дисциплины

| Планируемые результаты освоения ОП ВО (компетенции)                                                                       | Планируемые результаты обучения по дисциплине                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ОПК-10 Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности | Знает: основные понятия и задачи криптографии, математические модели криптографических систем; основные виды средств криптографической защиты информации (СКЗИ), включая блочные и поточные системы шифрования, криптографические системы с открытым ключом, криптографические хеш-функции и криптографические протоколы; национальные стандарты Российской Федерации в области криптографической защиты информации и сферы их применения<br>Умеет: использовать систему криптографической защиты информации (СКЗИ) для решения задач профессиональной деятельности |

## 3. Место дисциплины в структуре ОП ВО

| Перечень предшествующих дисциплин, видов работ учебного плана | Перечень последующих дисциплин, видов работ |
|---------------------------------------------------------------|---------------------------------------------|
| Нет                                                           | 1.О.41 Криптографические протоколы          |

Требования к «входным» знаниям, умениям, навыкам студента, необходимым при освоении данной дисциплины и приобретенным в результате освоения предшествующих дисциплин:

Нет

## 4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 3 з.е., 108 ч., 54,25 ч.  
контактной работы

| Вид учебной работы                                                         | Всего часов | Распределение по семестрам |
|----------------------------------------------------------------------------|-------------|----------------------------|
|                                                                            |             | в часах                    |
|                                                                            |             | Номер семестра             |
|                                                                            |             | 7                          |
| Общая трудоёмкость дисциплины                                              | 108         | 108                        |
| Аудиторные занятия:                                                        | 48          | 48                         |
| Лекции (Л)                                                                 | 16          | 16                         |
| Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ) | 32          | 32                         |
| Лабораторные работы (ЛР)                                                   | 0           | 0                          |
| Самостоятельная работа (СРС)                                               | 53,75       | 53,75                      |
| Подготовка к практическим занятиям. Выполнение домашних заданий            | 22          | 22                         |
| Подготовка к зачёту                                                        | 14          | 14                         |
| Написание программ, реализующих заданные криптоалгоритмы                   | 17,75       | 17.75                      |
| Консультации и промежуточная аттестация                                    | 6,25        | 6,25                       |
| Вид контроля (зачет, диф.зачет, экзамен)                                   | -           | зачет                      |

## 5. Содержание дисциплины

| № раздела | Наименование разделов дисциплины | Объем аудиторных занятий по видам в часах |   |    |    |
|-----------|----------------------------------|-------------------------------------------|---|----|----|
|           |                                  | Всего                                     | Л | ПЗ | ЛР |
| 1         | Введение в криптографию          | 4                                         | 2 | 2  | 0  |
| 2         | Криптосистемы с секретным ключом | 14                                        | 4 | 10 | 0  |
| 3         | Криптосистемы с открытым ключом  | 16                                        | 4 | 12 | 0  |
| 4         | Надежность шифров                | 2                                         | 2 | 0  | 0  |
| 5         | Алгоритмы цифровой подписи       | 10                                        | 2 | 8  | 0  |
| 6         | Современные стандарты шифрования | 2                                         | 2 | 0  | 0  |

### 5.1. Лекции

| № лекции | № раздела | Наименование или краткое содержание лекционного занятия                                                                                                                                                                                                                                                                                                                                                                                                                                    | Кол-во часов |
|----------|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| 2        | 1         | Исторический обзор. Открытые сообщения и их характеристики. История криптографии. Примеры ручных шифров. Основные этапы становления криптографии как науки. Частотные характеристики открытых текстов. Основные задачи и понятия криптографии. Перечень угроз. Симметричное и асимметричное шифрование в задачах защиты информации. Шифры с открытым ключом и их использование. Классификация шифров. Модели шифров. Основные требования к шифрам. Простейшие криптографические протоколы. | 2            |
| 4        | 2         | Поточные шифры замены Шифры простой замены и их анализ. Многоалфавитные шифры замены. Шифры гаммирования и их анализ. Использование неравновероятной гаммы, повторное использование гаммы, анализ шифра Виженера. Шифры перестановки Разновидности шифров                                                                                                                                                                                                                                  | 2            |

|    |   |                                                                                                                                                                                                                                                   |   |
|----|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
|    |   | перестановки: маршрутные и геометрические перестановки. Элементы анализа шифров перестановки.                                                                                                                                                     |   |
| 5  | 2 | Шифры Хилла. Шифры на основе псевдослучайных последовательностей. Линейные рекуррентные последовательности (ЛРП) над полем. Свойства ЛРП максимального периода. Линейная сложность псевдослучайной последовательности. Алгоритм Берлекемпа-Мессе. | 2 |
| 8  | 3 | «Public key cryptography»: Принцип построения шифрсистем с открытым ключом. Протокол Диффи-Хеллмана. Шифрсистема на основе задачи об «укладке рюкзака». Шифрсистема RSA. Шифрсистема Эль-Гамала.                                                  | 2 |
| 10 | 3 | Шифрсистема Нидеррайтера. Криптосистемы на основе эллиптических кривых.                                                                                                                                                                           | 2 |
| 13 | 4 | Основы теории К.Шеннона Криптографическая стойкость шифров. Теоретически стойкие шифры. Шифры, совершенные при нападении на открытый текст. Шифры, совершенные при нападении на ключ.                                                             | 2 |
| 16 | 5 | Общие требования к цифровой подписи. Цифровые подписи на основе шифрсистем с открытым ключом. Цифровая подпись Фиата-Шамира. Цифровая подпись Эль-Гамала. Стандарты цифровой подписи.                                                             | 2 |
| 17 | 6 | Современные блочные шифрсистемы. Сети Фейстеля. Криптоалгоритм DES. Криптоалгоритм RIJNDAEL. Криптоалгоритм ГОСТ-28147-89                                                                                                                         | 2 |

## 5.2. Практические занятия, семинары

| № занятия | № раздела | Наименование или краткое содержание практического занятия, семинара                        | Кол-во часов |
|-----------|-----------|--------------------------------------------------------------------------------------------|--------------|
| 1         | 1         | Шифры замены. Шифр Виженера. Перестановочные шифры. Шифры Хилла                            | 2            |
| 2         | 2         | Контрольная работа по симметричным криптосистемам                                          | 1            |
| 3         | 2         | Шифры на основе линейных рекуррентных последовательностей. Сети Фейстеля.                  | 6            |
| 4         | 2         | Контрольная работа по теме "Линейные рекуррентные последовательности"                      | 2            |
| 5         | 2         | Контрольная работа по теме "Сети Фейстеля"                                                 | 1            |
| 6         | 3         | Криптосистема на основе задачи о рюкзаке. Криптосистема RSA                                | 4            |
| 7         | 3         | Криптосистема Эль-Гамала. Эллиптические кривые. Шифрсистемы на основе эллиптических кривых | 4            |
| 8         | 3         | Контрольная работа по асимметричным системам шифрования.                                   | 2            |
| 9         | 3         | Элементы криптографического анализа.                                                       | 1            |
| 10        | 3         | Контрольная работа по теме "Криптографический анализ"                                      | 1            |
| 11        | 5         | Цифровая подпись Эль-Гамала.                                                               | 4            |
| 12        | 5         | Цифровая подпись Фиата-Шамира. Цифровая подпись Шнорра.                                    | 2            |
| 13        | 5         | Контрольная работа по теме "Цифровые подписи"                                              | 2            |

## 5.3. Лабораторные работы

Не предусмотрены

## 5.4. Самостоятельная работа студента

| Выполнение СРС                      |                                                                            |         |              |
|-------------------------------------|----------------------------------------------------------------------------|---------|--------------|
| Подвид СРС                          | Список литературы (с указанием разделов, глав, страниц) / ссылка на ресурс | Семестр | Кол-во часов |
| Подготовка к практическим занятиям. | Глухов М.М. Введение в теоретико-                                          | 7       | 22           |

|                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |   |       |
|----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|-------|
| Выполнение домашних заданий                              | числовые методы в криптографии. -- СПб. : Лань, 2011. — 400 с.<br><a href="http://e.lanbook.com/">http://e.lanbook.com/</a> Голиков, А.М. Методы шифрования информации в сетях и системах радиосвязи. [Электронный ресурс] — Электрон. дан. — М. : ТУСУР, 2012. — 329 с. <a href="http://e.lanbook.com/">http://e.lanbook.com/</a> Рябко, Б.Я. Основы современной криптографии и стеганографии. [Электронный ресурс] / Б.Я. Рябко, А.Н. Фионов. — Электрон. дан. — М. : Горячая линия-Телеком, 2013. — 232 с. <a href="http://e.lanbook.com/">http://e.lanbook.com/</a>                                  |   |       |
| Подготовка к зачёту                                      | Глухов М.М. Введение в теоретико-числовые методы в криптографии. -- СПб. : Лань, 2011. — 400 с.<br><a href="http://e.lanbook.com/">http://e.lanbook.com/</a> Голиков, А.М. Методы шифрования информации в сетях и системах радиосвязи. [Электронный ресурс] — Электрон. дан. — М. : ТУСУР, 2012. — 329 с. <a href="http://e.lanbook.com/">http://e.lanbook.com/</a> Рябко, Б.Я. Основы современной криптографии и стеганографии. [Электронный ресурс] / Б.Я. Рябко, А.Н. Фионов. — Электрон. дан. — М. : Горячая линия-Телеком, 2013. — 232 с. <a href="http://e.lanbook.com/">http://e.lanbook.com/</a> | 7 | 14    |
| Написание программ, реализующих заданные криптоалгоритмы | Глухов М.М. Введение в теоретико-числовые методы в криптографии. -- СПб. : Лань, 2011. — 400 с.<br><a href="http://e.lanbook.com/">http://e.lanbook.com/</a> Голиков, А.М. Методы шифрования информации в сетях и системах радиосвязи. [Электронный ресурс] — Электрон. дан. — М. : ТУСУР, 2012. — 329 с. <a href="http://e.lanbook.com/">http://e.lanbook.com/</a> Рябко, Б.Я. Основы современной криптографии и стеганографии. [Электронный ресурс] / Б.Я. Рябко, А.Н. Фионов. — Электрон. дан. — М. : Горячая линия-Телеком, 2013. — 232 с. <a href="http://e.lanbook.com/">http://e.lanbook.com/</a> | 7 | 17,75 |

## 6. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации

Контроль качества освоения образовательной программы осуществляется в соответствии с Положением о балльно-рейтинговой системе оценивания результатов учебной деятельности обучающихся.

### 6.1. Контрольные мероприятия (КМ)

| № КМ | Се-местр | Вид контроля | Название контрольного мероприятия | Вес | Макс. балл | Порядок начисления баллов           | Учитывается в ПА |
|------|----------|--------------|-----------------------------------|-----|------------|-------------------------------------|------------------|
| 1    | 7        | Текущий      | Контрольная работа                | 1   | 15         | 15 баллов - задача решена правильно | зачет            |

|   |   |                          |                                                              |   |    |                                                                                                                                                                                                                                                                                                                            |       |
|---|---|--------------------------|--------------------------------------------------------------|---|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|   |   | контроль                 | "Симметричные криптографические системы"                     |   |    | 10-14 баллов - в решение есть неточности и незначительные ошибки<br>6-9 баллов - общий ход решения верен, но имеются серьёзные недочёты<br>3-5 баллов - в решении присутствует ряд серьёзных ошибок<br>1-2 баллов - есть некоторый намёк на решение<br>0 баллов - задача не решалась                                       |       |
| 2 | 7 | Текущий контроль         | Контрольная работа "Шифры на основе ЛРП"                     | 1 | 15 | 15 баллов - задача решена правильно<br>10-14 баллов - в решение есть неточности и незначительные ошибки<br>6-9 баллов - общий ход решения верен, но имеются серьёзные недочёты<br>3-5 баллов - в решении присутствует ряд серьёзных ошибок<br>1-2 балла - есть некоторый намёк на решение<br>0 баллов - задача не решалась | зачет |
| 3 | 7 | Текущий контроль         | Контрольная работа "Сети Фейстеля"                           | 1 | 5  | 5 баллов - задача решена правильно<br>4 балла - в решение есть неточности и незначительные ошибки<br>3 балла - общий ход решения верен, но имеются серьёзные недочёты<br>2 балла - в решении присутствует ряд серьёзных ошибок<br>1 балл - есть некоторый намёк на решение<br>0 баллов - задача не решалась                | зачет |
| 4 | 7 | Текущий контроль         | Контрольная работа "Асимметричные криптографические системы" | 1 | 15 | 15 баллов - задача решена правильно<br>10-14 баллов - в решение есть неточности и незначительные ошибки<br>6-9 баллов - общий ход решения верен, но имеются серьёзные недочёты<br>3-5 баллов - в решении присутствует ряд серьёзных ошибок<br>1-2 балла - есть некоторый намёк на решение<br>0 баллов - задача не решалась | зачет |
| 5 | 7 | Промежуточная аттестация | Конспект лекций                                              | - | 10 | 10 баллов - конспект представлен в полном объёме<br>6-9 баллов - имеется около 3/4 от всего объёма лекций<br>1-5 баллов - имеется 1/2 от всего объёма лекций<br>0 баллов - имеется менее половины объёма всех лекций                                                                                                       | зачет |
| 6 | 7 | Промежуточная аттестация | Зачёт                                                        | - | 40 | 40 баллов - задача решена правильно<br>30-39 баллов - в решение есть неточности и незначительные ошибки<br>20-29 баллов - общий ход решения верен, но имеются серьёзные недочёты<br>10-19 балла - в решении присутствует ряд серьёзных ошибок<br>1-9 балл - есть некоторый намёк на                                        | зачет |

|  |  |  |  |  |                                          |  |
|--|--|--|--|--|------------------------------------------|--|
|  |  |  |  |  | решение<br>0 баллов - задача не решалась |  |
|--|--|--|--|--|------------------------------------------|--|

## 6.2. Процедура проведения, критерии оценивания

| Вид промежуточной аттестации | Процедура проведения                                                                                                                                                                                                                                                                                                                                                                                         | Критерии оценивания                     |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|
| зачет                        | При оценивании результата мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.19 N 179). На зачёте происходит оценивание учебной деятельности на основе оценок за мероприятия текущего контроля. Студент может улучшить свой рейтинг пройдя мероприятие текущей аттестации, которое не является обязательным. | В соответствии с пп. 2.5, 2.6 Положения |

## 6.3. Паспорт фонда оценочных средств

| Компетенции | Результаты обучения                                                                                                                                                                                                                                                                                                                                                                                                                       | № КМ |   |   |   |   |   |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---|---|---|---|---|
|             |                                                                                                                                                                                                                                                                                                                                                                                                                                           | 1    | 2 | 3 | 4 | 5 | 6 |
| ОПК-10      | Знает: основные понятия и задачи криптографии, математические модели криптографических систем; основные виды средств криптографической защиты информации (СКЗИ), включая блочные и поточные системы шифрования, криптографические системы с открытым ключом, криптографические хеш-функции и криптографические протоколы; национальные стандарты Российской Федерации в области криптографической защиты информации и сферы их применения | +    | + | + | + | + | + |
| ОПК-10      | Умеет: использовать систему криптографической защиты информации (СКЗИ) для решения задач профессиональной деятельности                                                                                                                                                                                                                                                                                                                    | +    | + | + | + | + | + |

Типовые контрольные задания по каждому мероприятию находятся в приложениях.

## 7. Учебно-методическое и информационное обеспечение дисциплины

### Печатная учебно-методическая документация

*а) основная литература:*

Не предусмотрена

*б) дополнительная литература:*

Не предусмотрена

*в) отечественные и зарубежные журналы по дисциплине, имеющиеся в библиотеке:*

Не предусмотрены

*г) методические указания для студентов по освоению дисциплины:*

1. Зюляркина Н.Д. Криптографические методы защиты информации.  
Методические указания по проведению практических занятий

*из них: учебно-методическое обеспечение самостоятельной работы студента:*

## Электронная учебно-методическая документация

| № | Вид литературы            | Наименование ресурса в электронной форме          | Библиографическое описание                                                                                                                                                                                                           |
|---|---------------------------|---------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Основная литература       | Электронно-библиотечная система издательства Лань | Глухов М.М. Введение в теоретико-числовые методы в криптографии. -- СПб. : Лань, 2011. — 400 с. <a href="http://e.lanbook.com/">http://e.lanbook.com/</a>                                                                            |
| 2 | Дополнительная литература | Электронно-библиотечная система издательства Лань | Голиков, А.М. Методы шифрования информации в сетях и системах радиосвязи. [Электронный ресурс] — Электрон. дан. — М. : ТУСУР, 2012. — 329 с. <a href="http://e.lanbook.com/">http://e.lanbook.com/</a>                               |
| 3 | Основная литература       | Электронно-библиотечная система издательства Лань | Рябко, Б.Я. Основы современной криптографии и стеганографии. [Электронный ресурс] / Б.Я. Рябко, А.Н. Фионов. — Электрон. дан. — М. : Горячая линия-Телеком, 2013. — 232 с. <a href="http://e.lanbook.com/">http://e.lanbook.com/</a> |

Перечень используемого программного обеспечения:

Нет

Перечень используемых профессиональных баз данных и информационных справочных систем:

Нет

## 8. Материально-техническое обеспечение дисциплины

| Вид занятий                     | № ауд.   | Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий                                                                                                                                                           |
|---------------------------------|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Лабораторные занятия            | 913 (36) | Комплект компьютерного оборудования; Локальная вычислительная сеть; Коммутатор, Программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozilla Firefox, Консультант+; Локальные СЗИ: Secret Net 6.5 (автономный вариант), Страж 3.0; Межсетевые экраны: ViPNet Custom 3.1, User Gate 5.2 |
| Практические занятия и семинары | 913 (36) | Комплект компьютерного оборудования; Локальная вычислительная сеть; Коммутатор, Программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozilla Firefox, Консультант+; Локальные СЗИ: Secret Net 6.5 (автономный вариант), Страж 3.0; Межсетевые экраны: ViPNet Custom 3.1, User Gate 5.2 |
| Лекции                          | 912 (36) | Комплект компьютерного оборудования, LCD Проектор, Экран проекционный, настенные стенды по защите информации (5 шт. ), программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozilla Firefox, Консультант+.                                                                             |