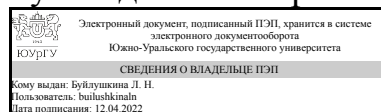


# ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:  
Руководитель направления



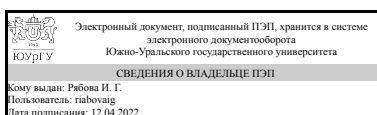
Л. Н. Буйлушкина

## РАБОЧАЯ ПРОГРАММА

дисциплины 1.О.17 Организационная защита информации  
для направления 09.03.04 Программная инженерия  
уровень Бакалавриат  
форма обучения очная  
кафедра-разработчик Гуманитарные, естественно-научные и технические дисциплины

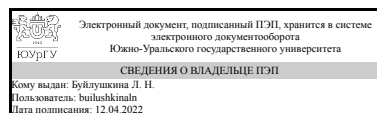
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 09.03.04 Программная инженерия, утверждённым приказом Минобрнауки от 19.09.2017 № 920

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



И. Г. Рябова

Разработчик программы,  
старший преподаватель



Л. Н. Буйлушкина

## 1. Цели и задачи дисциплины

Целью дисциплины «Организационная защита информации» является: - изучение основных направлений защиты компьютерной информации; - изучение организационных и административных методов защиты информации; - изучение программно-аппаратных средств защиты компьютерных систем; - обзор готовых решений по обеспечению информационной безопасности, разработка программных средств аудита безопасности, выявления вторжений и программных средств криптографической защиты информации. Задачами дисциплины являются: - дать знания студентам по основным угрозам безопасности компьютерных систем; - дать знания основных стандартов безопасности компьютерных систем; - дать знания моделей безопасности компьютерных систем; - дать знания основных криптографических систем; - дать знания основ администрирования сетей и защиты информации в сетях.

## Краткое содержание дисциплины

Основы информационной безопасности и защита информации. История криптографии. Основные термины и определения. Классификация шифров. Шифры замены. Шифры перестановки. Шифры гаммирования. Комбинированные шифры. Шифрование с открытым ключом. Хеш-функции. Криптографические протоколы. протоколы обмена ключами. Протоколы аутентификации (идентификации). Протоколы электронной цифровой подписи. Протоколы контроля целостности. Протоколы электронных платежей. Протоколы голосования. Другие протоколы. Некоторые сведения из теорий алгоритмов и чисел. Основы криптоанализа. Стеганография. Кодирование информации.

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

| Планируемые результаты освоения ОП ВО (компетенции)                                                                                                                                                                                             | Планируемые результаты обучения по дисциплине                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | Знает: основные нормативные правовые акты в области обеспечения информационной безопасности; основные принципы функционирования компьютерных сетей; сетевую модель TCP/IP и OSI; принципы коммутации в LAN сетях; принципы маршрутизации в LAN и WAN сетях; технологии шифрования и авторизации<br>Умеет: применять действующую законодательную базу в области обеспечения информационной безопасности; читать справочную литературу по телекоммуникационным сетям и применять на практике; использовать CIDR, разбивать и складывать сети; конфигурировать VLAN и планировать коммутацию в LAN сети; работать с таблицами маршрутизации; планировать списки контроля доступа; конфигурирование AAA (аутентификации, авторизации и аудита); организовывать туннелирование с шифрованием |

|                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                 | Имеет практический опыт: владения профессиональной терминологией в области информационной безопасности; настройки и конфигурирования STP, VLAN; настройка и конфигурирование статической и динамической маршрутизации; настройки механизма NAT и PAT; настройка ACL списков                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| ОПК-4 Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью | <p>Знает: основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем. Принципы организации защиты информации; подходы к построению модели нарушителя и объекта с точки зрения информационной безопасности. Основы организационного и правового обеспечения информационной безопасности.</p> <p>Умеет: обосновать принципы организации технического, программного и информационного обеспечения информационной безопасности; применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации</p> <p>Имеет практический опыт: применения навыков работы с нормативными правовыми актами; применения навыков работы с нормативными документами; применения навыков организации и обеспечения режима секретности.</p> |

### 3. Место дисциплины в структуре ОП ВО

| Перечень предшествующих дисциплин, видов работ учебного плана                                                                                                                                                                                                                                                                                  | Перечень последующих дисциплин, видов работ |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------|
| 1.О.12.02 Инженерная графика,<br>1.О.12.01 Начертательная геометрия,<br>1.О.16 Метрология, стандартизация и сертификация,<br>Учебная практика, технологическая (проектно-технологическая) практика (2 семестр),<br>Учебная практика, научно-исследовательская работа (получение первичных навыков научно-исследовательской работы) (4 семестр) | Не предусмотрены                            |

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

| Дисциплина                   | Требования                                                                                                                |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| 1.О.12.02 Инженерная графика | Знает: требования стандартов Единой системы конструкторской документации (ЕСКД) и Единой системы технической документации |

|                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                    | <p>(ЕСТД) к оформлению и составлению чертежей, методы проецирования и построения изображений геометрических фигур; принципы графического изображения деталей и узлов; основные правила построения и чтения чертежей технических объектов, правила оформления графических и текстовых документов в соответствии с требованиями ЕСКД; методы решения инженерно-геометрических задач на чертеже; правила выполнения чертежей деталей, сборочных единиц; Умеет: анализировать форму предметов в натуре и по чертежам; моделировать предметы по их изображениям; применять современные стандарты и средства проектирования, использовать законы начертательной геометрии и проекционного черчения при дальнейшем обучении и для решения профессиональных инженерных задач; на основе методов построения изображений геометрических фигур решать различные позиционные и метрические задачи, относящиеся к этим фигурам Имеет практический опыт: выполнения и чтения чертежей и электрических схем, а также составления спецификаций в соответствии со стандартами ЕСКД, решения метрических задач, пространственных объектов на чертежах; применения методов проецирования и изображения пространственных форм на плоскости проекций</p> |
| 1.О.12.01 Начертательная геометрия | <p>Знает: основы оформления чертежей и эскизов деталей и документации; основные требования, предъявляемые к технической документации, материалам, изделиям; основные положения конструкторской документации, основные законы геометрического формирования, построения и взаимного пересечения моделей плоскости и пространства, необходимые для выполнения и чтения чертежей; методы построения обратимых чертежей пространственных объектов; Умеет: самостоятельно использовать конструкторскую и технологическую документацию в объеме достаточном для решения профессиональных задач; выполнять чертежи деталей, оставить цель и выбрать пути её достижения; воспринимать оптимальное соотношение частей и целого на основе графических моделей, практически реализуемых в виде чертежей конкретных пространственных объектов; решать метрические и позиционные задачи; использовать полученные графические знания и навыки в различных отраслях профессиональной деятельности; конструировать образы из геометрических поверхностей Имеет практический опыт: применения типовых</p>                                                                                                                                             |

|                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                             | <p>методов и способов выполнения и разработки проектно-конструкторской документации; применения аналитических и графических методов и способов выполнения и разработки проектно-конструкторской документации; работы в графических редакторах , применения способов проецирования и изображения пространственных объектов; применение методов преобразования геометрических тел</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 1.О.16 Метрология, стандартизация и сертификация                                                                            | <p>Знает: современные стандарты и средства проектирования, разработки и тестирования прикладного ПО; основные стандарты в области метрологии, стандартизации и сертификации; структуру документов и нормативные требования к их составлению, теорию, средства и виды измерений, метрологическое обеспечение стандартизации и сертификации, средства и виды измерений, схемы прямых и косвенных измерений, источники и классификация погрешностей, государственную систему стандартизации, международные стандарты; принципы стандартизации, принципы стандартизации в технической сфере, лицензирование Умеет: применять современные стандарты и средства проектирования, разработки и тестирования прикладного ПО; применять в профессиональной деятельности основные стандарты по метрологии, стандартизации и сертификации; разрабатывать технические задания на создание подсистем информационной безопасности, использовать стандарты и другие нормативные документы по обеспечению качества выполняемых работ; планировать и выполнять метрологические и сертификационные испытания Имеет практический опыт: применения современных стандартов и средств проектирования, разработки и тестирования прикладного ПО; составления программной отчетности в соответствии с требованиями и стандартами оформления и содержания; владения терминологией в области метрологии, стандартизации и сертификации; владения навыками работы с документами; применения инструментальных средств анализа (моделирования) проекта и решения типовых задач профессиональной направленности; применения инструментальных средств управления проектом на всех этапах его жизненного цикла.</p> |
| Учебная практика, научно-исследовательская работа (получение первичных навыков научно-исследовательской работы) (4 семестр) | <p>Знает: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

|  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <p>информационной безопасности, основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы, современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности., основы системного администрирования, современные стандарты информационного взаимодействия систем, теоретические основы поиска, хранения, и анализа информации, основы программирования, проектирования, конструирования и тестирования программных продуктов, основные концепции, принципы и факты, связанные с информатикой, основные языки программирования, современные программные среды разработки информационных систем и технологий</p> <p>Умеет: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности, применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы, выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности, выполнять параметрическую настройку информационных и автоматизированных систем., применять методы поиска и хранения информации с использованием современных информационных технологий, применять парадигмы программирования к проектированию, конструированию и тестированию программных продуктов, применять основные концепции, принципы и факты, связанные с информатикой, в практической деятельности., применять языки программирования, современные программные среды разработки информационных систем и технологий для автоматизации бизнес-процессов, решения прикладных задач различных классов</p> <p>Имеет практический опыт: подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно- исследовательской работе с учетом требований информационной безопасности, составления технической документации на различных этапах жизненного цикла информационной системы, применения современных информационных технологий и программных средств, в том числе</p> |
|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                          | <p>отечественного производства, при решении задач профессиональной деятельности, инсталляции программного и аппаратного обеспечения информационных и автоматизированных систем, поиска, хранения и анализа информации с использованием современных информационных технологий, программирования и тестирования программных продуктов, применения основных концепций, принципов и фактов, связанные с информатикой, в профессиональной деятельности, программирования, отладки и тестирования прототипов программно-технических комплексов задач</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <p>Учебная практика, технологическая (проектно-технологическая) практика (2 семестр)</p> | <p>Знает: современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности., основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы, основные языки программирования, современные программные среды разработки информационных систем и технологий, принципы сбора, отбора и обобщения информации, основные концепции, принципы и факты, связанные с информатикой, принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности, теоретические основы поиска, хранения, и анализа информации, основы системного администрирования, современные стандарты информационного взаимодействия систем</p> <p>Умеет: выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности, применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы, применять языки программирования, современные программные среды разработки информационных систем и технологий для автоматизации бизнес-процессов, решения прикладных задач различных классов, соотносить разнородные явления и систематизировать их в рамках избранных видов профессиональной деятельности, применять основные концепции, принципы и факты, связанные с информатикой, в практической деятельности., решать стандартные задачи профессиональной деятельности на основе</p> |

|  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <p>информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности, применять методы поиска и хранения информации с использованием современных информационных технологий, выполнять параметрическую настройку информационных и автоматизированных систем. Имеет практический опыт: применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности, составления технической документации на различных этапах жизненного цикла информационной системы, программирования, отладки и тестирования прототипов программно-технических комплексов задач, работы с информационными источниками, опыт научного поиска, создания научных текстов, применения основных концепций, принципов и фактов, связанные с информатикой, в профессиональной деятельности, подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности, поиска, хранения и анализа информации с использованием современных информационных технологий, инсталляции программного и аппаратного обеспечения информационных и автоматизированных систем</p> |
|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### 4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 3 з.е., 108 ч., 48,25 ч.  
контактной работы

| Вид учебной работы                                                         | Всего часов | Распределение по семестрам в часах |
|----------------------------------------------------------------------------|-------------|------------------------------------|
|                                                                            |             | Номер семестра                     |
|                                                                            |             | 7                                  |
| Общая трудоёмкость дисциплины                                              | 108         | 108                                |
| <i>Аудиторные занятия:</i>                                                 | 48          | 48                                 |
| Лекции (Л)                                                                 | 32          | 32                                 |
| Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ) | 16          | 16                                 |
| Лабораторные работы (ЛР)                                                   | 0           | 0                                  |
| <i>Самостоятельная работа (СРС)</i>                                        | 53,75       | 53,75                              |
| с применением дистанционных образовательных технологий                     | 0           |                                    |

|                                          |       |       |
|------------------------------------------|-------|-------|
| Подготовка реферата, презентации         | 33,75 | 33.75 |
| Подготовка к зачету                      | 20    | 20    |
| 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         | Основы информационной безопасности и защита информации.                                                                                  | 6                                         | 4 | 2  | 0  |
| 2         | История криптографии. Основные термины и определения. Классификация шифров                                                               | 6                                         | 4 | 2  | 0  |
| 3         | Шифры замены. Шифры перестановки. Шифры гаммирования. Комбинированные шифры. Шифрование с открытым ключом.                               | 8                                         | 6 | 2  | 0  |
| 4         | Хеш-функции.                                                                                                                             | 6                                         | 4 | 2  | 0  |
| 5         | Криптографические протоколы. протоколы обмена ключами. Протоколы аутентификации (идентификации). Протоколы электронной цифровой подписи. | 10                                        | 6 | 4  | 0  |
| 6         | Протоколы контроля целостности. Протоколы электронных платежей. Протоколы голосования. Другие протоколы.                                 | 6                                         | 4 | 2  | 0  |
| 7         | Некоторые сведения из теорий алгоритмов и чисел. Основы криптоанализа. Стеганография. Кодирование информации.                            | 6                                         | 4 | 2  | 0  |

### 5.1. Лекции

| № лекции | № раздела | Наименование или краткое содержание лекционного занятия                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Кол-во часов |
|----------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| 1,2      | 1         | Основы информационной безопасности: Информация и информационная безопасность, основные составляющие информационной безопасности, объекты защиты, категории и носители информации, средства защиты информации.                                                                                                                                                                                                                                                                                                                                                                           | 4            |
| 3,4      | 2         | История криптографии: Наивная криптография, формальная криптография, математическая криптография. Основные термины и определения: Классификация шифров. Основные термины и определения, основные требования к криптосистемам, классификация криптографических систем.                                                                                                                                                                                                                                                                                                                   | 4            |
| 5,6,7    | 3         | Шифры замены: Основы шифрования, шифры: однозначной замены, полиалфавитные, омофонические, полиалфавитные. Шифры перестановки: Основы шифрования, шифры одинарной и множественной перестановки. Шифры гаммирования: Основы шифрования, шифрование по модулю N и 2, генерация гаммы, генераторы гамм. Комбинированные шифры: Основы шифрования, ADFGX, DES, ГОСТ 28147-89. Шифрование с открытым ключом: Основы шифрования, алгоритм RSA, алгоритм на основе задачи об укладке ранца, вероятностное шифрование, алгоритм шифрования Эль-Гамала, алгоритм на основе эллиптических кривых. | 6            |
| 8,9      | 4         | Хеш-функции: Основные понятия, MD5, применение шифрования для получения хеш-образа                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 4            |
| 10,11,12 | 5         | Криптографические протоколы. протоколы обмена ключами: Основные сведения о криптографических протоколах, протоколы обмена ключами. Протоколы аутентификации (идентификации): Общие сведения, парольная идентификация / аутентификация, протокол идентификации /                                                                                                                                                                                                                                                                                                                         | 6            |

|       |   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |   |
|-------|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
|       |   | аутентификации с использованием хеш-функции, протокол идентификации / аутентификации на основе шифрования с открытым ключом, сервер аутентификации Kerberos, идентификация / аутентификация с помощью биометрических данных, идентификационные карты (ID-cards) и электронные ключи. Протоколы электронной цифровой подписи: Общие сведения, протокол на базе алгоритма RSA, алгоритм цифровой подписи ГОСТ 34.10-94, алгоритм цифровой подписи ГОСТ 34.10-2001, разновидности ЭЦП.                                                                                                                                                                                                     |   |
| 13,14 | 6 | Протоколы контроля целостности: Общие сведения, использование контрольных сумм, использование ЭЦП, использование MAC-кодов, проверка четности, использование ECC, комбинированные методы. Протоколы электронных платежей: Общие сведения, пластиковые карты, суррогатные платежные средства в Internet, расчеты пластиковыми карточками в Internet, электронные кошельки в Internet, цифровые деньги. Протоколы голосования: Общие сведения, некоторые варианты реализации протоколов электронного голосования, российский опыт электронного голосования. Другие протоколы: Протокол разделения секрета, протокол подбрасывания монеты "по телефону", тайные многосторонние вычисления. | 4 |
| 15,16 | 7 | Некоторые сведения из теорий алгоритмов и чисел: Сложность алгоритмов, простые числа, разложение числа на простые сомножители, нахождение начального списка простых чисел, тестирование числа на простоту, определение наибольшего общего делителя. Основы криптоанализа: Угрозы безопасности при использовании криптографии, общие сведения о криптоанализе, разновидности атак на криптосистемы. Стеганография: Общие сведения, классическая стеганография, компьютерная стеганография. Кодирование информации: Общие сведения, общедоступные и секретные кодовые системы, номенклатуры.                                                                                              | 4 |

## 5.2. Практические занятия, семинары

| № занятия | № раздела | Наименование или краткое содержание практического занятия, семинара                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Кол-во часов |
|-----------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| 1         | 1         | Основы информационной безопасности: Информация и информационная безопасность, основные составляющие информационной безопасности, объекты защиты, категории и носители информации, средства защиты информации.                                                                                                                                                                                                                                                                                                                                                                           | 2            |
| 2         | 2         | История криптографии: Наивная криптография, формальная криптография, математическая криптография. Основные термины и определения: Классификация шифров. Основные термины и определения, основные требования к криптосистемам, классификация криптографических систем.                                                                                                                                                                                                                                                                                                                   | 2            |
| 3         | 3         | Шифры замены: Основы шифрования, шифры: однозначной замены, полиалфавитные, омофонические, полиалфавитные. Шифры перестановки: Основы шифрования, шифры одинарной и множественной перестановки. Шифры гаммирования: Основы шифрования, шифрование по модулю N и 2, генерация гаммы, генераторы гамм. Комбинированные шифры: Основы шифрования, ADFGX, DES, ГОСТ 28147-89. Шифрование с открытым ключом: Основы шифрования, алгоритм RSA, алгоритм на основе задачи об укладке ранца, вероятностное шифрование, алгоритм шифрования Эль-Гамала, алгоритм на основе эллиптических кривых. | 2            |
| 4         | 4         | Хеш-функции: Основные понятия, MD5, применение шифрования для получения хеш-образа                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2            |
| 5,6       | 5         | Криптографические протоколы. протоколы обмена ключами: Основные сведения о криптографических протоколах, протоколы обмена ключами. Протоколы аутентификации (идентификации): Общие сведения, парольная                                                                                                                                                                                                                                                                                                                                                                                  | 4            |

|   |   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |   |
|---|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
|   |   | идентификация / аутентификация, протокол идентификации / аутентификации с использованием хеш-функции, протокол идентификации / аутентификации на основе шифрования с открытым ключом, сервер аутентификации Kerberos, идентификация / аутентификация с помощью биометрических данных, идентификационные карты (ID-cards) и электронные ключи. Протоколы электронной цифровой подписи: Общие сведения, протокол на базе алгоритма RSA, алгоритм цифровой подписи ГОСТ 34.10-94, алгоритм цифровой подписи ГОСТ 34.10-2001, разновидности ЭЦП.                                                                                                                                            |   |
| 7 | 6 | Протоколы контроля целостности: Общие сведения, использование контрольных сумм, использование ЭЦП, использование MAC-кодов, проверка четности, использование ECC, комбинированные методы. Протоколы электронных платежей: Общие сведения, пластиковые карты, суррогатные платежные средства в Internet, расчеты пластиковыми карточками в Internet, электронные кошельки в Internet, цифровые деньги. Протоколы голосования: Общие сведения, некоторые варианты реализации протоколов электронного голосования, российский опыт электронного голосования. Другие протоколы: Протокол разделения секрета, протокол подбрасывания монеты "по телефону", тайные многосторонние вычисления. | 2 |
| 8 | 7 | Некоторые сведения из теорий алгоритмов и чисел: Сложность алгоритмов, простые числа, разложение числа на простые сомножители, нахождение начального списка простых чисел, тестирование числа на простоту, определение наибольшего общего делителя. Основы криптоанализа: Угрозы безопасности при использовании криптографии, общие сведения о криптоанализе, разновидности атак на криптосистемы. Стеганография: Общие сведения, классическая стеганография, компьютерная стеганография. Кодирование информации: Общие сведения, общедоступные и секретные кодовые системы, номенклатуры.                                                                                              | 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 реферата, презентации | ЭУМД ОСН. 1 стр. 25-65; стр. 75-87; стр. 111-130; стр. 93-101; стр. 183-210; ЭУМД доп. 1 стр. 41-95; стр. 131-148                      | 7       | 33,75        |
| Подготовка к зачету              | ЭУМД ОСН. 1 стр. 25-65; стр. 75-87; стр. 111-130; стр. 93-101; стр. 183-210; ЭУМД осн. 2 стр. 7-14; стр. 15-39 ЭУМД доп. 1 стр. 41-51; | 7       | 20           |

## 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 контроль         | Шифрование, дешифрование информации с применением комбинированных криптографических алгоритмов | 1   | 15         | 13-15 баллов - практические навыки работы с освоенным материалом полностью сформированы 11-13 баллов - практические навыки работы с освоенным материалом сформированы недостаточно 9-11 баллов - необходимые практические навыки работы с освоенным материалом в основном сформированы  | зачет            |
| 2    | 7        | Текущий контроль         | Режимы работы блочных шифров. Схемы кратного шифрования                                        | 1   | 15         | 13-15 баллов - практические навыки работы с освоенным материалом полностью сформированы 11- 13 баллов - практические навыки работы с освоенным материалом сформированы недостаточно 9-11 баллов - необходимые практические навыки работы с освоенным материалом в основном сформированы | зачет            |
| 3    | 7        | Текущий контроль         | Дешифрование заданной фразы с применением известного криптографического алгоритма              | 1   | 15         | 13-15 баллов - практические навыки работы с освоенным материалом полностью сформированы 11-13 баллов - практические навыки работы с освоенным материалом сформированы недостаточно 9-11 баллов - необходимые практические навыки работы с освоенным материалом в основном сформированы  | зачет            |
| 4    | 7        | Текущий контроль         | Программная реализация криптографических протоколов                                            | 1   | 15         | 13-15 баллов - практические навыки работы с освоенным материалом полностью сформированы 11- 13 баллов - практические навыки работы с освоенным материалом сформированы недостаточно 9-11 баллов - необходимые практические навыки работы с освоенным материалом в основном сформированы | зачет            |
| 5    | 7        | Промежуточная аттестация | Зачет                                                                                          | -   | 30         | студенты в аудитории индивидуально отвечают на теоретические вопросы, которые включают вопросы по пройденным разделам, преподаватель беседует и оценивает. 17-30 баллов оценка Зачтено: знает основной материал дисциплины; верно излагает и интерпретирует знания; изложение           | зачет            |

|  |  |  |  |  |  |                                                                                                                                                                                                                                                                                    |  |
|--|--|--|--|--|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
|  |  |  |  |  |  | материала логически выстроено. Менее 17 баллов оценка Не зачтено: не знает значительной части материала дисциплины; ответ не дан или допускает грубые ошибки при изложении ответа на вопрос; неверно излагает и интерпретирует знания; изложение материала логически не выстроено. |  |
|--|--|--|--|--|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|

## 6.2. Процедура проведения, критерии оценивания

| Вид промежуточной аттестации | Процедура проведения                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Критерии оценивания                     |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|
| зачет                        | на зачете происходит оценивание учебной деятельности обучающихся по дисциплине на основе полученных оценок за контрольно-рейтинговые мероприятия текущего контроля.<br>При оценивании результатов учебной деятельности обучающегося по дисциплине используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утв. приказом ректора от 24.05.2019 № 179) Зачтено: рейтинг обучающегося за мероприятие больше или равен 60%. Не зачтено: рейтинг обучающегося за мероприятие меньше 60% | В соответствии с пп. 2.5, 2.6 Положения |

## 6.3. Паспорт фонда оценочных средств

| Компетенции | Результаты обучения                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | № КМ |   |   |   |   |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---|---|---|---|
|             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 1    | 2 | 3 | 4 | 5 |
| ОПК-3       | Знает: основные нормативные правовые акты в области обеспечения информационной безопасности; основные принципы функционирования компьютерных сетей; сетевую модель TCP/IP и OSI; принципы коммутации в LAN сетях; принципы маршрутизации в LAN и WAN сетях; технологии шифрования и авторизации                                                                                                                                                                                      | +    |   | + |   | + |
| ОПК-3       | Умеет: применять действующую законодательную базу в области обеспечения информационной безопасности; читать справочную литературу по телекоммуникационным сетям и применять на практике; использовать CIDR, разбивать и складывать сети; конфигурировать VLAN и планировать коммутацию в LAN сети; работать с таблицами маршрутизации; планировать списки контроля доступа; конфигурирование AAA (аутентификации, авторизации и аудита); организовывать туннелирование с шифрованием | +    |   | + |   | + |
| ОПК-3       | Имеет практический опыт: владения профессиональной терминологией в области информационной безопасности; настройки и конфигурирования STP, VLAN; настройка и конфигурирование статической и динамической маршрутизации; настройки механизма NAT и PAT; настройка ACL списков                                                                                                                                                                                                          | +    |   | + |   | + |
| ОПК-4       | Знает: основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем. Принципы организации защиты информации; подходы к построению модели нарушителя и объекта с точки зрения информационной безопасности. Основы организационного и правового обеспечения информационной безопасности.                                                                                                                                    |      | + |   | + | + |
| ОПК-4       | Умеет: обосновать принципы организации технического, программного и информационного обеспечения информационной безопасности; применять                                                                                                                                                                                                                                                                                                                                               |      | + |   | + | + |

|       |                                                                                                                                                                                                                                                |   |  |  |   |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|--|--|---|
|       | нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации |   |  |  |   |
| ОПК-4 | Имеет практический опыт: применения навыков работы с нормативными правовыми актами; применения навыков работы с нормативными документами; применения навыков организации и обеспечения режима секретности.                                     | + |  |  | + |

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:

1. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей [Текст]/ В.Ф. Шаньгин.- М.: ИД «ФОРУМ»: ИНФРА-М, 2011.- 416 с. - ISBN 978-5 8199-0331-5
2. Малюк, А.А. Введение в защиту информации в автоматизированных системах [Текст]: учебное пособие для вузов / А.А. Малюк, С.В. Пазизин, Н.С.Погожин. – 2-е изд. – М.: Горячая линия – Телеком, 2004. – 147с.: ил.- ISBN 5-93517-062-0.
3. Хорев, П.Б. Методы и средства защиты информации в компьютерных системах [Текст]: учебное пособие для студентов вузов / П.Б. Хорев.- М.: Академия, 2006.- 256с.- ISBN 5-7695-1839-1.

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

1. Программирование

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

1. Защита информации и криптография: методические указания по выполнению самостоятельной работы для обучающихся по направлению 09.03.04 Программная инженерия / сост. Л.Н.Буйлушкина – Нижневартонск, 2022. – 11 с.

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

1. Защита информации и криптография: методические указания по выполнению самостоятельной работы для обучающихся по направлению 09.03.04 Программная инженерия / сост. Л.Н.Буйлушкина – Нижневартонск, 2022. – 11 с.

### Электронная учебно-методическая документация

| № | Вид литературы | Наименование ресурса в электронной форме | Библиографическое описание |
|---|----------------|------------------------------------------|----------------------------|
|---|----------------|------------------------------------------|----------------------------|

|   |                           |                                                   |                                                                                                                                                                                                                                                                                           |
|---|---------------------------|---------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Основная литература       | Электронно-библиотечная система издательства Лань | Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. <a href="https://e.lanbook.com/book/156401">https://e.lanbook.com/book/156401</a>                      |
| 2 | Основная литература       | Электронно-библиотечная система издательства Лань | Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии : учебник / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2019. — 344 с. — ISBN 978-5-8114-3940-9. <a href="https://e.lanbook.com/book/125739">https://e.lanbook.com/book/125739</a> |
| 3 | Дополнительная литература | Электронно-библиотечная система Znanium.com       | Глинская, Е. В. Информационная безопасность конструкций ЭВМ и систем : учеб. пособие / Е.В. Глинская, Н.В. Чичварин. — Москва : ИНФРА-М, 2019. — 118 с. <a href="https://new.znanium.com/read?id=327864">https://new.znanium.com/read?id=327864</a>                                       |
| 4 | Дополнительная литература | Электронно-библиотечная система Znanium.com       | Баранова, Е.В. Информационная безопасность и защита информации : учеб. пособие / Баранова Е.К., Бабаев А.В. — 4-е изд., перераб. и доп. — М. : РИОР : ИНФРА-М, 2019. — 336 с. <a href="https://new.znanium.com/read?id=336219">https://new.znanium.com/read?id=336219</a>                 |

Перечень используемого программного обеспечения:

1. Microsoft-Office(бессрочно)
2. ФГАОУ ВО "ЮУрГУ (НИУ)"-Портал "Электронный ЮУрГУ" (<https://edu.susu.ru>)(бессрочно)
3. -Borland Developer Studio(бессрочно)

Перечень используемых профессиональных баз данных и информационных справочных систем:

1. -Консультант Плюс (Нижневартовск)(бессрочно)

## 8. Материально-техническое обеспечение дисциплины

| Вид занятий                     | № ауд. | Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий                                                                                          |
|---------------------------------|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Лекции                          |        | Занятия студентов проходят в лекционных и компьютерных аудиториях филиала. Основная и дополнительная литература, словари находятся в фондах библиотеки филиала, где также организован доступ к материалам электронных библиотечных систем |
| Практические занятия и семинары |        | Предустановленное программное обеспечение: ОС Windows 7 Professional; Денвер; MS SQL Server 2008R2; Oracle VM VirtualBox; Microsoft Office 2010; Информационно-правовая база «Консультант – Плюс»; DOSBox                                 |