Министерство науки и высшего образования Российской Федерации

**федеральное государственное бюджетное образовательное учреждение высшего образования**
**РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ**

Кафедра Информационных технологий и систем безопасности

Рабочая программа по дисциплине

# КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Основная профессиональная образовательная программа
высшего образования программы специалитета по специальности

**10.05.02 «Информационная безопасность телекоммуникационных систем»**

Специализация:
**Разработка защищенных телекоммуникационных систем**

Квалификация:
**Специалист**

Форма обучения
**Очная**

**Согласовано**
**Руководитель ОПОП**
**«Информационная безопасность телекоммуникационных систем»**
_____ **Бурлов В.Г.**

**Утверждаю**
**Председатель УМС** _____ **И.И. Палкин**

**Рекомендована решением**
**Учебно-методического совета**
**«11» июня 2019 г., протокол № 7**

**Рассмотрена и утверждена на заседании кафедры**
**«07» мая 2019 г., протокол № 5**
**Зав. кафедрой** _____ **Завгородний В.Н.**

**Авторы-разработчики:**
_____ **Татарникова Т.М.**

Санкт-Петербург 2019

## 1. Цели освоения дисциплины

**Целью** освоения дисциплины «Криптографические методы защиты информации» является ознакомление с основополагающими принципами защиты информации с использованием криптографических методов и примерами реализации этих методов на практике, формирование у обучаемых предметной компетентности и творческого мышления.

**Задачи дисциплины – дать основы:**

– системного подхода в организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов;

– принципов синтеза и анализа шифров; математических методов, используемых в криптоанализе.

## 2. Место дисциплины в структуре ОП

Дисциплина «Криптографические методы защиты информации» для направления подготовки 10.05.02 – информационная безопасность телекоммуникационных систем относиться к дисциплинам базовой части блока1 дисциплины (модули) (Б1.Б.10).

Для освоения дисциплины «Криптографические методы защиты информации», необходимо обладать базовыми знаниями (общее среднее образование), а также освоить учебный материал предшествующих дисциплин:

– «Информационные технологии»,
– «Теория вероятностей и математическая статистика»,
– «Дискретная математика»,
– «Теория информации и кодирования»,
– «Информатика и программирование»,
– «Основы информационной безопасности».

Параллельно с дисциплиной «Криптографические методы защиты информации» изучаются дисциплины: «Системы и сети передачи информации», «Аппаратные средства телекоммуникационных систем», «Цифровая обработка сигналов», «ГИС технологии в ТКС», «Телекоммуникационные системы».

Знания и практики, полученные обучаемыми по дисциплине «Криптографические методы защиты информации», непосредственно используются для подготовки дипломного проекта и в практической профессиональной деятельности, связанной с защитой информации от утечки по техническим каналам.

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

Процесс изучения дисциплины направлен на формирование следующих компетенций:

| Код компетенции | Компетенция |
|---|---|
| ОПК-3 | способность применять положения теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов, информации и кодирования, электрической связи для решения профессиональных задач |
| ПК-5 | способность проектировать защищённые телекоммуникационные системы и их элементы, проводить анализ проектных решений по обеспечению заданного уровня безопасности и требуемого качества обслуживания, разрабатывать необходимую техническую документацию с учетом действующих нормативных и методических документов |
| ПК-8 | способность проводить анализ эффективности технических и программно-аппаратных средств защиты телекоммуникационных систем |
| ПСК-7.5 | способность обеспечивать защиту программных средств защищенных телекоммуникационных систем |

В результате освоения компетенций в рамках дисциплины «Криптографические методы защиты информации» обучающийся должен:

| Код компетенции | Результаты обучения |
|---|---|
| ОПК-3 | **Знать:** основные классы шифров, сложность их реализации;<br>**Уметь:** применять математические методы описания и исследования криптосистем;<br>**Владеть:** навыками использования основных типов шифров и криптографических алгоритмов при решении задач обеспечения информационной безопасности; |
| ПК-5 | **Знать:** основные криптографические протоколы систем шифрования с открытым ключом и закрытым ключом;<br>**Уметь:** проектировать криптографические протоколы для защищенных телекоммуникационных систем и их элементов; проводить анализ проектных решений по обеспечению заданного уровня безопасности и требуемого качества обслуживания;<br>**Владеть:** методами оценки криптографической стойкости алгоритмов шифрования; |
| ПК-8 | **Знать:** типовые поточные и блочные шифры, а также асимметричные криптосистемы;<br>**Уметь:** оценивать криптографическую стойкость шифров;<br>**Владеть:** методами оценки криптографической стойкости шифров; |
| ПСК-7.5 | **Знать:** программно-аппаратные средства реализации криптографических систем защиты информации;<br>**Уметь:** применять математические методы описания и исследования криптосистем;<br>**Владеть:** криптографическими средствами и базовыми технологиями информационной безопасности; |

Основные признаки проявленности формируемых компетенций в результате освоения дисциплины «Защита операционных систем» сведены в таблице.

| Уровень освоения компетенции | Результат обучения | Результат обучения | Результат обучения | Результат обучения |
|---|---|---|---|---|
| | ОПК-3: Знать, уметь, владеть | ПК-5: Знать, уметь, владеть | ПК-8: Знать, уметь, владеть | ПСК-7.5: Знать, уметь, владеть |
| минимальный | Владеет основными навыками работы с источниками и критической литературой | Владеет основными навыками работы с источниками и критической литературой | Владеет основными навыками работы с источниками и критической литературой | Владеет основными навыками работы с источниками и критической литературой |
| | Способен представить ключевую проблему в ее связи с другими процессами | Способен представить ключевую проблему в ее связи с другими процессами | Способен представить ключевую проблему в ее связи с другими процессами | Способен представить ключевую проблему в ее связи с другими процессами |
| | Понимает специфику основных рабочих категорий | Понимает специфику основных рабочих категорий | Понимает специфику основных рабочих категорий | Понимает специфику основных рабочих категорий |
| базовый | Свободно излагает материал, однако не демонстрирует навыков сравнения основных идей и концепций | Свободно излагает материал, однако не демонстрирует навыков сравнения основных идей и концепций | Свободно излагает материал, однако не демонстрирует навыков сравнения основных идей и концепций | Свободно излагает материал, однако не демонстрирует навыков сравнения основных идей концепций |
| | Способен выделить и сравнить концепции, но испытывает сложности с их практической привязкой | Способен выделить и сравнить концепции, но испытывает сложности с их практической привязкой | Способен выделить и сравнить концепции, но испытывает сложности с их практической привязкой | Способен выделить и сравнить концепции, но испытывает сложности с их практической привязкой |
| | Знает основные отличия концепций в заданной проблемной области | Знает основные отличия концепций в заданной проблемной области | Знает основные отличия концепций в заданной проблемной области | Знает основные отличия концепций в заданной проблемной области |
| продвинутый | Видит источники современных проблем в заданной области анализа, владеет подходами к их решению | Видит источники современных проблем в заданной области анализа, владеет подходами к их решению | Видит источники современных проблем в заданной области анализа, владеет подходами к их решению | Видит источники современных проблем в заданной области анализа, владеет подходами к их решению |
| | Выявляет основания заданной области анализа, понимает ее практическую ценность, однако испытывает затруднения в описании сложных объектов анализа | Выявляет основания заданной области анализа, понимает ее практическую ценность, однако испытывает затруднения в описании сложных объектов анализа | Выявляет основания заданной области анализа, понимает ее практическую ценность, однако испытывает затруднения в описании сложных объектов анализа | Выявляет основания заданной области анализа, понимает ее практическую ценность, однако испытывает затруднения объектов анализа |

| | | | | |
|---|---|---|---|---|
| | Знает основное содержание современных научных идей в рабочей области анализа, способен их сопоставить | Знает основное содержание современных научных идей в рабочей области анализа, способен их сопоставить | Знает основное содержание современных научных идей в рабочей области анализа, способен их сопоставить | Знает основное содержание современных научных идей в рабочей области анализа, способен их сопоставить |

**Соответствие уровней освоения компетенции планируемым результатам обучения и критериям их оценивания**

| Этап (уровень) освоения компетенции | Основные признаки проявленности компетенции (дескрипторное описание уровня) | | | | |
|---|---|---|---|---|---|
| | 1. | 2. | 3. | 4. | 5. |
| минимальный | не владеет | слабо ориентируется в терминологии и содержании | Способен выделить основные идеи текста, работает с критической литературой | Владеет основными навыками работы с источниками и критической литературой | Способен дать собственную критическую оценку изучаемого материала |
| | не умеет | не выделяет основные идеи | Способен показать основную идею в развитии | Способен представить ключевую проблему в ее связи с другими процессами | Может соотнести основные идеи с современными проблемами |
| | не знает | допускает грубые ошибки | Знает основные рабочие категории, однако не ориентируется в их специфике | Понимает специфику основных рабочих категорий | Способен выделить характерный авторский подход |
| базовый | не владеет | плохо ориентируется в терминологии и содержании | Владеет приемами поиска и систематизации, но не способен свободно изложить материал | Свободно излагает материал, однако не демонстрирует навыков сравнения основных идей и концепций | Способен сравнивать концепции, аргументированно излагает материал |
| | не умеет | выделяет основные идеи, но не видит проблем | Выделяет конкретную проблему, однако излишне упрощает ее | Способен выделить и сравнить концепции, но испытывает сложности с их практической привязкой | Аргументированно проводит сравнение концепций по заданной проблематике |
| | не знает | допускает много ошибок | Может изложить основные рабочие категории | Знает основные отличия концепций в заданной проблемной области | Способен выделить специфику концепций в заданной проблемной области |
| продвинутый | не владеет | ориентируется в терминологии и содержании | В общих чертах понимает основную идею, однако плохо связывает ее с существующей проблематикой | Видит источники современных проблем в заданной области анализа, владеет подходами к их решению | Способен грамотно обосновать собственную позицию относительно решения современных проблем в заданной области |
| | не умеет | выделяет основные идеи, но не видит их в развитии | Может понять практическое назначение основной идеи, но затрудняется выявить ее основания | Выявляет основания заданной области анализа, понимает ее практическую ценность, однако испытывает затруднения в описании сложных объектов анализа | Свободно ориентируется в заданной области анализа. Понимает ее основания и умеет выделить практическое значение заданной области |
| | не знает | допускает ошибки при выделении рабочей области анализа | Способен изложить основное содержание современных научных идей в рабочей области анализа | Знает основное содержание современных научных идей в рабочей области анализа, способен их сопоставить | Может дать критический анализ современным проблемам в заданной области анализа |

## 4. Структура и содержание дисциплины

Общая трудоемкость (объем) дисциплины (модуля) составляет 5 зачетные единицы (ЗЕ*), 180 академических часа.

*Объем дисциплины Криптографические методы защиты информации по видам учебных занятий в академических часах*)

| **Объём дисциплины** | **Всего часов** |
|---|---|
| | **Очная форма обучения** |
| **Общая трудоёмкость дисциплины** | 180 |
| **Контактная работа обучающихся с преподавателем (по видам аудиторных учебных занятий) – всего:** | 74 |
| в том числе: | |
| лекции | 30 |
| практические занятия | 14 |
| лабораторные занятия | 30 |
| **Самостоятельная работа** (СРС), всего: | 106 |
| экзамен | 18 |
| **Вид промежуточной аттестации (зачет/экзамен)** | экзамен |

### 4.1.Структура дисциплины

| № п/п | Раздел и тема дисциплины | Семестр | Виды учебной работы, в т.ч. самостоятельная работа студентов, час. | | | Формы текущего контроля успеваемости | Занятия в активной и интерактивной форме, час. | Формируемые компетенции |
|---|---|---|---|---|---|---|---|---|
| | | | Лекции | Лаборат. Практич. | Самост. работа | | | |
| 1 | Введение в криптографические методы защиты информации | 6 | 4 | 6 | 14 | Отчеты по лабораторным работам | 10/6 | ОПК-3 ПК-5 ПК-8 ПСК-7.5 |
| 2 | Способы формирования криптограмм | 6 | 4 | 8 | 14 | Отчеты по лабораторным работам | 12/8 | ОПК-3 ПК-5 ПК-8 ПСК-7.5 |
| 3 | Симметричные с криптосистемы | 6 | 8 | 10 | 24 | Отчеты по лабораторным работам | 18/10 | ОПК-3 ПК-5 ПК-8 ПСК-7.5 |
| 4 | Асимметричные криптосистемы | 6 | 6 | 10 | 24 | Отчеты по лабораторным работам | 16/10 | ОПК-3 ПК-5 ПК-8 ПСК-7.5 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 5 | Приложение криптографии | 6 | 8 | 10 | 30 | Отчеты по лабораторным работам | 18/10 | ОПК-3<br>ПК-5<br>ПК-8<br>ПСК-7.5 |
| | **ИТОГО** | | 30 | 44 | 106 | | 74/44 | |

## 4.2. Содержание разделов дисциплины

### 4.2.1. Введение в криптографические методы защиты информации

Информация как объект защиты. Базовая криптографическая система, ее элементы и функции. Криптография, как наука шифрования данных и криптоанализа. Классификация шифров. Краткие сведения из теории чисел, применяемой в криптографии: модульная арифметика, теорема Эйлера, теорема Ферма, возведение в степень, вычисление дискретного логарифма, разложение на множители, вычисление наибольшего общего делителя, обращение элементов по модулю, тесты на простоту.

Модели шифрования/дешифрования дискретных сообщений. Понятие стойкость криптосистемы .

Краткая история развития криптографии: простейшие шифры и их свойства, шифры замены и перестановки, шифр Цезаря, квадрат Полибия, решетка «Кардано», табло Вижинера, шифр Плейфейера, шифровальный аппарат Вернама, зарождение цифровой криптографии, основные этапы становления криптографии как науки.

### 4.2.2. Способы формирования криптограмм

Блоковое шифрование: основные обратимые и необратимые криптопримитивы, схемы образования блочных шифров с помощью сетей, многократное шифрование блоков.

Потоковые шифры: аддитивные шифры и применение линейных рекуррентных регистров для потокового шифрования.

### 4.2.3. Симметричные криптосистемы

Аппаратное шифрование DES. Криптоалгоритмы: TEA, IDEA, ГОСТ 28147-89. Алгоритмы конкурса AES: MARS, RC6, Rijndael, TwoFish, Serpent. Итоги конкурса AES.

### 4.2.4. Асимметричные криптосистемы

Особенности асимметричных криптосистем. Требования к практически реализуемым криптосистемам с открытым ключом. Основы построения асимметричных систем. Распределение ключей в асимметричной криптосистеме. Гибридная система шифрования.

Практические схемы асимметричного шифрования: криптоалгоритмы RSA, Рабина, Эль Гамаль, Мак-Элиса.

### 4.2.5. Приложение криптографии

Электронная цифровая подпись. Хеширование. Обеспечение безопасности электронных платежей

Методы и средства обеспечения подлинности информации: обобщенная система электронной цифровой подписи (ЭЦП). ЭЦП RSA, ЭЦП Рабина, ЭЦП Эль Гамаль, ЭЦП DSA, ЭЦП ГОСТ Р 34.10-2001.

Хэш-функции: однонаправленные хэш-функции на основе симметричных блочных алгоритмов; самостоятельные хэш-алгоритмы: MD5, SHA-1, ГОСТ Р 34.11-94

### 4.3. Семинарские, практические, лабораторные занятия, их содержание

| № п/п | № раздела дисциплины | Тема занятия | Форма проведения | Формируемые компетенции |
|---|---|---|---|---|
| 1 | 1 | Задачи информационной безопасности | Практическое занятие | ОПК-3<br>ПК-5<br>ПК-8<br>ПСК-7.5 |
| 2 | 1 | Исторические шифры | Лабораторная работа | ОПК-3<br>ПК-5<br>ПК-8<br>ПСК-7.5 |
| 3 | 1 | Криптографическая защита информации. Представление информации в цифровом виде. | Практическое занятие | ОПК-3<br>ПК-5<br>ПК-8<br>ПСК-7.5 |
| 4 | 1 | Исследование шифров многобуквенной замены | Лабораторная работа | ОПК-3<br>ПК-5<br>ПК-8<br>ПСК-7.5 |
| 5 | 2 | Принципы построения блоковых шифров. Свойства смешивания и рассеивания. | Практическая занятие | ОПК-3<br>ПК-5<br>ПК-8<br>ПСК-7.5 |
| 6 | 2 | Основные задачи в области управления ключами | Практическое занятие | ОПК-3<br>ПК-5<br>ПК-8<br>ПСК-7.5 |
| 7 | 2 | Блочное симметричное шифрование | Лабораторная работа | ОПК-3<br>ПК-5<br>ПК-8<br>ПСК-7.5 |
| 8 | 2 | Шифр гаммирования | Лабораторная работа | ОПК-3<br>ПК-5<br>ПК-8<br>ПСК-7.5 |
| 9 | 2 | Методы построения больших периодов в поточных шифрах. Регистры сдвига с линейной | Практическое занятие | ОПК-3<br>ПК-5<br>ПК-8 |

| | | | | |
|---|---|---|---|---|
| | | обратной связью (РСЛОС) | | ПСК-7.5 |
| 10 | 3 | Криптографические сети | Лабораторная работа | ОПК-3<br>ПК-5<br>ПК-8<br>ПСК-7.5 |
| 11 | 4 | Математические основы систем с открытым ключом Модульная арифметика. Алгоритм Евклида и его сложность | Практическое занятие | ОПК-3<br>ПК-5<br>ПК-8<br>ПСК-7.5 |
| 12 | 4 | Асимметричные криптосистемы | Лабораторная работа | ОПК-3<br>ПК-5<br>ПК-8<br>ПСК-7.5 |
| 13 | 5 | Криптографические хэш-функции | Лабораторная работа | ОПК-3<br>ПК-5<br>ПК-8<br>ПСК-7.5 |
| 14 | 5 | Протоколы разделения секрета | Практическое занятие | ОПК-3<br>ПК-5<br>ПК-8<br>ПСК-7.5 |
| 15 | 5 | Алгоритмы электронной цифровой подписи | Лабораторная работа | ОПК-3<br>ПК-5<br>ПК-8<br>ПСК-7.5 |

## 5. Учебно-методическое обеспечение самостоятельной работы студент и оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

### 5.1. Текущий контроль

Текущий контроль производится путем защиты лабораторных работ.

***Критерии оценивания лабораторных работ.***

– оценка «зачтено»: работа полностью выполнена. Даны полные ответы на вопросы по теме работы;

– оценка «не зачтено»: работа не выполнена или при защите студент не может ясно и четко ответить на поставленные вопросы.

### 5.2. Методические указания по организации самостоятельной работы

Во время самостоятельной работы студенты знакомятся с существующими методами исследования технических каналов утечки информации и характеристик технических средств защиты информации от ее утечки по техническим каналам, читают методические указания по выполнению лабораторных работ, читают дополнительный материал в виде лекционных занятий, работают с методическими указаниями по написанию курсовой работы.

В перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине «Криптографические методы защиты информации» входит:

– Методические указания по выполнению лабораторных работ.
– Дополнительный лекционный материал.

***Контроль исполнения*** самостоятельных работ осуществляется преподавателем с участием студентов в форме обсуждения выполненных заданий и работ.

**5.3. Промежуточный контроль: экзамен**

**Перечень вопросов для промежуточной аттестации (экзамен):**

1. Сети блочных шифров, их основные параметры. SP-сеть, KASLT-сеть.
2. Шифры одноалфавитной замены. Шифр Цезаря, квадрат «Полибия». Сравнительные характеристики.
3. История развития криптографии. Особенности периодов развития.
4. Определение блочного шифрования. Блок информации. Ключ алгоритма. Абсолютно симметричный блочный шифр.
5. Динамический поточный шифр
6. Концепция шифрования на открытом ключе.
7. Концепция шифрования на закрытом ключе
8. Понятие хэш-функции. Общая схема образования хэш-функции.
9. Классификация шифров по ключевой информации.
10. Нелинейные лоточные шифры. Фильтрующие шифры. Линейный регистр сдвига.
11. Аппаратное шифрование DES: структура, перестановки, сеть Файстеля, расширение ключа.
12. Классическая структура сети Файстеля. Ветви сети, материал ключа, раунд сети, образующая функция.
13. Комбинирующие поточные шифры. Корреляционно-стойкий комбинирующий шифр.
14. Абсолютно симметричная сеть Файстеля. Модификация сети Файстеля дня большего числа ветвей: тип 1.
15. Комбинирующий поточный шифр с элементом памяти
16. Модификация сети Файстеля дня большего числа ветвей: тип 2 и тип 3. 1
17. Шифры многоалфавитной замены. Табло Виженера
18. Понятие стойкости криптосистемы. Виды криптоанализа
19. ЭЦП RSA
20. ЭЦП Эль-Гамаль
21. Обратимые операции в блочном шифровании. 22. ЭЦП ГОСТ Р 34.10-2001
23. Базовая модель криптографии.
24. Хэш-функция MD5
25. Асимметричное шифрование алгоритмом Рабина
26. Асимметричное шифрование RSA
27. Асимметричная шифрование Эль-Гамаль

28. TEA: структура, алгоритм, образующая функция, ключ.
29. ЭЦП Рабина
30. Хэш-функции на основе блочного шифрования.
31. Необратимые операции в блочном шифровании.
32. Шифры перестановки. Квадрат «Кардана».
33. MARS структура: образующая функция, схемы входного и выходного перемешивания.
34. Алгоритм Rijndael.
35. IDEA: структура, алгоритм, расширение ключа.
36. Конкурс AES: цели и условия конкурса, алгоритмы шифрования конкурса.
37. Схема многократного шифрования блоков информации
38. Аддитивные потоковые шифры.
39. Обеспечение подлинности информации. Общая схема ЭЦП.
40. Основные принципы шифрования на открытом ключе.

**Образец билета:**

**Экзаменационный билет № 1**

1) Определение блочного шифрования. Блок информации. Ключ алгоритма. Абсолютно симметричный блочный шифр.

2) Хэш-функция MD5.

Заведующий кафедрой /_____/

***Критерии оценивания:***

Оценка «отлично» ставится студенту, ответ которого содержит:

•глубокое знание программного материала, а также основного содержания и новаций лекционного курса по сравнению с учебной литературой;

•знание концептуально-понятийного аппарата всего курса; а также свидетельствует о способности:

•самостоятельно критически оценивать основные положения курса;

•увязывать теорию с практикой.

Оценка «отлично» не ставится в случаях систематических пропусков студентом семинарских и лабораторных занятий по неуважительным причинам, а также неправильных ответов на дополнительные вопросы преподавателя.

Оценка «хорошо» ставится студенту, ответ которого свидетельствует о полном знании материала по программе, а также содержит в целом правильное, но не всегда точное и аргументированное изложение материала.

Оценка «хорошо» не ставится в случаях систематических пропусков студентом семинарских и практических занятий по неуважительным причинам, а также неправильных ответов на дополнительные вопросы преподавателя.

Оценка «удовлетворительно» ставится студенту, ответ которого содержит:

•поверхностные знания важнейших разделов программы и содержания лекционного курса;

•затруднения с использованием научно-понятийного аппарата и терминологии курса;

•стремление логически четко построить ответ, а также свидетельствует о возможности последующего обучения.

Оценка «неудовлетворительно» ставится студенту, имеющему существенные пробелы в знании основного материала по программе, а также допустившему принципиальные ошибки при изложении материала

**6. Учебно-методическое и информационное обеспечение дисциплины**

**а) основная литература:**

1. Бабенко, Л. К. Криптографическая защита информации: симметричное шифрование: учебное пособие для вузов / Л. К. Бабенко, Е. А. Ищукова. – М.: Издательство Юрайт, 2018. – 220 с. – (Серия : Университеты России). – ISBN 978-5-9916-9244-1. – Режим доступа: www.biblio-online.ru/book/6946C235-8650-4A29-B75B-68E0EF829422.

2. Криптографические методы защиты информации. Ч. 1. Основы криптографии. [Текст]: учебное пособие / П. П. Бескид, Татарникова Т.М.; РГГМУ. – Санкт-Петербург: РГГМУ, 2010. – 94 с. – 70.40 р.

3. Криптографические методы защиты информации. Ч. 2. Алгоритмы, методы и средства обеспечения конфиденциальности, подлинности и целостности информации [Текст]: учебное пособие / П. П. Бескид, Татарникова Т.М.; РГГМУ. – Санкт-Петербург: РГГМУ, 2010. – 103 с. – 77.00 р.

4. Криптографическая защита информации: учеб. пособие [Электронный ресурс] / С.О. Крамаров, О.Ю. Митясова, С.В. Соколов [и др.]; под ред. проф. С.О. Крамарова. – М.: РИОР: ИНФРА-М, 2018. – 321 с. – (Высшее образование). – Режим доступа: http://znanium.com/bookread2.php?book=901659

**б) дополнительная литература:**

1. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты: учебник для академического бакалавриата / В. М. Фомичёв, Д. А. Мельников; под ред. В. М. Фомичёва. – М.: Издательство Юрайт, 2018. – 245 с. – (Серия: Бакалавр. Академический курс). – ISBN 978-5-9916-7090-6. – Режим доступа: www.biblio-online.ru/book/AF99BBDE-AF3A-43A9-A90F-B99806553C25

2. Васильева, И. Н. Криптографические методы защиты информации: учебник и практикум для академического бакалавриата / И. Н. Васильева. – М. : Издательство Юрайт, 2018. – 349 с. – (Серия : Бакалавр. Академический курс). — ISBN 978-5-534-02883-6. – Режим доступа: www.biblio-online.ru/book/59BABD78-5536-4ED4-BB9D-55E2F19F80B2.

3. Криптографические методы защиты информации [Текст]: лабораторный практикум / Т. М. Татарникова; РГГМУ. – Санкт-Петербург: РГГМУ, 2013. – 63 с. – 23.02 р.

4. Криптографические методы защиты информации. [Текст]: методические

указания к выполнению лабораторных работ / Т. М. Татарникова; РГГМУ. – Санкт-Петербург: РГГМУ, 2010. – 50 с. – 50.00 р.

**в) программное обеспечение и Интернет-ресурсы:**

*Программное обеспечение:*

- windows 7
- office 2007
- dr Web
- Scilab 6.0.1 GNU General Public License 2.0
- Dev-C++ GNU General Public License

*Интернет-ресурсы*

- https://210fz.ru/fz-ob-informacionnoj-bezopasnosti/ - законы РФ по информационной безопасности
- http://geoline-tech.com/top-20-sites-about-information-security - ГеоЛайнТехнологии (интернет ресурсы для специалистов по информационной безопасности)
- https://compress.ru/technology – КомпьютерПресс (технологии, информационная безопасность, сети ТКС …)

*Информационно-справочные системы:*

- https://biblio-online.ru – ЭБС Юрайт
- http://znanium.com – ЭБС Знаниум
- http://www.prospektnauki.ru – ЭБС Проспект науки
- http://elib.rshu.ru ЭБС ГидроМетеоОнлайн
- https://нэб.рф - Национальная электронная библиотека

*Профессиональные базы данных*

- База данных Web of Science
- База данных Scopus
- Электронно-библиотечная система elibrary

## 7. Методические указания для обучающихся по освоению дисциплины (модуля)

| Вид занятия | Организация деятельности студента |
|---|---|
| Лекция | Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на лабораторном занятии. |

| | |
|---|---|
| Лабораторные | На лабораторных занятиях выполняются лабораторные работы по овладению методами экспериментальных исследований технических каналов утечки информации и характеристик технических средств защиты информации от ее утечки по техническим каналам, изученные во время лекций. Как правило, на каждом занятии студент должен показать результаты выполнения лабораторной преподавателю. |
| Внеаудиторная работа | представляет собой вид занятий, которые каждый студент организует и планирует самостоятельно. Самостоятельная работа студентов включает самостоятельное изучение разделов дисциплины. |
| Подготовка к зачёту/экзамену | При подготовке к экзамену необходимо ориентироваться на конспекты лекций, рекомендуемую литературу и др. |

## 8. Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

| Тема (раздел) дисциплины | Образовательные и информационные технологии | Перечень программного обеспечения и информационных справочных систем |
|---|---|---|
| Введение в криптографические методы защиты информации | Лабораторные работы<br>Практические занятия<br>Технология объяснительно-иллюстративного обучения | https://biblio-online.ru<br>http://znanium.com<br>http://www.prospektnauki.ru<br>http://elib.rshu.ru<br>https://нэб.рф<br>windows 7<br>office 2007<br>dr Web<br>Scilab 6.0.1 GNU<br>Dev-C++ GNU |
| Способы формирования криптограмм | Лабораторные работы<br>Практические занятия<br>Технология объяснительно-иллюстративного обучения | https://biblio-online.ru<br>http://znanium.com<br>http://www.prospektnauki.ru<br>http://elib.rshu.ru<br>https://нэб.рф<br>windows 7<br>office 2007<br>dr Web<br>Scilab 6.0.1 GNU<br>Dev-C++ GNU |
| Симметричные криптосистемы | Лабораторные работы<br>Практические занятия<br>Технология объяснительно-иллюстративного обучения | https://biblio-online.ru<br>http://znanium.com<br>http://www.prospektnauki.ru<br>http://elib.rshu.ru<br>https://нэб.рф<br>windows 7<br>office 2007<br>dr Web<br>Scilab 6.0.1 GNU<br>Dev-C++ GNU |
| Асимметричные криптосистемы | Лабораторные работы<br>Практические занятия<br>Технология объяснительно- | https://biblio-online.ru<br>http://znanium.com<br>http://www.prospektnauki.ru |

| | | |
|---|---|---|
| | иллюстративного обучения | http://elib.rshu.ru<br>https://нэб.рф<br>windows 7<br>office 2007<br>dr Web<br>Scilab 6.0.1 GNU<br>Dev-C++ GNU |
| Приложения криптографии | Лабораторные работы<br>Практические занятия<br>Технология объяснительно-иллюстративного обучения | https://biblio-online.ru<br>http://znanium.com<br>http://www.prospektnauki.ru<br>http://elib.rshu.ru<br>https://нэб.рф<br>windows 7<br>office 2007<br>dr Web<br>Scilab 6.0.1 GNU<br>Dev-C++ GNU |

## 9. Особенности освоения дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Обучение обучающихся с ограниченными возможностями здоровья при необходимости осуществляется на основе адаптированной рабочей программы с использованием специальных методов обучения и дидактических материалов, составленных с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся (обучающегося).

При определении формы проведения занятий с обучающимся-инвалидом учитываются рекомендации, содержащиеся в индивидуальной программе реабилитации инвалида, относительно рекомендованных условий и видов труда.

При необходимости для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья создаются специальные рабочие места с учетом нарушенных функций и ограничений жизнедеятельности.

## 10. Материально-техническое обеспечение дисциплины

Учебная аудитории для проведения занятий лекционного типа – укомплектована специализированной (учебной) мебелью, набором демонстрационного оборудования и учебно-наглядными пособиями, обеспечивающими тематические иллюстрации, соответствующие рабочим учебным программам дисциплин (модулей).

Учебная аудитории для проведения занятий практического типа – укомплектована специализированной (учебной) мебелью, набором демонстрационного оборудования и учебно-наглядными пособиями, обеспечивающими тематические иллюстрации, соответствующие рабочим учебным программам дисциплин (модулей).

Учебная аудитория для групповых и индивидуальных консультаций - укомплектована специализированной (учебной) мебелью, техническими средствами обучения, служащими для представления учебной информации.

Помещение для самостоятельной работы – укомплектовано

специализированной (учебной) мебелью, оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечено доступом в электронную информационно-образовательную среду организации

Помещение для хранения и профилактического обслуживания учебного оборудования – укомплектовано специализированной мебелью для хранения оборудования и техническими средствами для его обслуживания.

Лаборатория – компьютерный класс с ЛВС связанной с интернетом и мультимедиа.