Министерство образования и науки Российской Федерации

федеральное государственное бюджетное образовательное учреждение высшего образования
РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

Кафедра Морских информационных систем

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
«___» _____ 2018 г., протокол №___

Рассмотрена и утверждена на заседании кафедры
13 мая 2018 г., протокол № 05/18
и.о. зав. кафедрой _____ **Завгородний**

Авторы-разработчики:
_____ **Яготинцева Н.В.**

Санкт-Петербург 2018

Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ
УНИВЕРСИТЕТ

РАБОЧАЯ ПРОГРАММА
дисциплины
«Криптографические методы защиты информации»

Направление подготовки
10.05.02 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Профиль: Разработка защищенных телекоммуникационных систем

Квалификация (степень)
СПЕЦИАЛИСТ

РГГМУ

Санкт– Петербург
2015

Рекомендована Учёным советом факультета Информационных систем и геотехнологий РГГМУ
(Протокол №___ от ___ _____ 201_ г.)

Программа дисциплины «Криптографические методы защиты информации». Направление подготовки 10.05.02 – информационная безопасность телекоммуникационных систем. Профиль: Разработка защищенных телекоммуникационных систем. Квалификация (степень) – СПЕЦАЛИСТ. Для высших учебных заведений. – СПб.: Изд. РГГМУ, 2015 – 15 с.

Составили: Шапаренко Ю.М. – к.т.н. доцент кафедры Информационных технологий и систем безопасности. Яготинцева Н.В. – ассистент кафедры Информационных технологий и систем безопасности.

Ответственный редактор: Бескид П.П. – заведующий кафедрой Информационных технологий и систем безопасности. Российского государственного гидрометеорологического университета.

Рецензент: федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения», профессор кафедры безопасности информационных систем, д.т.н., профессор Татарникова Т. М.

© Ю.М. Шапаренко, Н.В. Яготинцева, 2015.
© Российский государственный гидрометеорологический университет (РГГМУ), 2015.

1. Цели освоения дисциплины

Целью освоения дисциплины «Криптографические методы защиты информации» является изложение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике, формирование у обучаемых предметной компетентности и творческого мышления.

.

.**Задачи дисциплины – дать основы:**

– системного подхода к 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 блока дисциплин (модулей) (Б1.Б.10) профессионального цикла.

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»,

-«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: – возможности технических средств перехвата информации; Уметь: – применять математические методы описания и исследования криптосистем; Владеть: – навыками использования основных типов шифров и криптографических алгоритмов;
ПК-5	Знать: – частотные характеристики открытых текстов и их применение к анализу простейших симметричных криптосистем; – основные криптографические протоколы системы шифрования с открытыми ключами; Уметь: – проектировать защищённые телекоммуникационные системы и их элементы – проводить анализ проектных решений по обеспечению заданного уровня безопасности и требуемого качества обслуживания Владеть: – методами криптоанализа простейших шифров; – методами оценки криптографической стойкости алгоритмов шифрования;
ПК-8	Знать – типовые поточные и блочные шифры, а также асимметричные криптосистемы; Уметь: – оценивать криптографическую стойкость шифров Владеть: – профессиональной терминологией в области информационной безопасности;
ПСК-7.5	Знать: – криптографические средства и системы защиты информации и их программно-аппаратную реализацию; Уметь: – применять математические методы описания и исследования криптосистем;

	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** ОПК-3: Знать, уметь, владеть	**Результат обучения** ПК-5: Знать, уметь, владеть	**Результат обучения** ПК-8: Знать, уметь, владеть	**Результат обучения** 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 и 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 в описании сложных 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	Способен изложить основное	Знает основное содержание	Может дать критический

		при выделении рабочей области анализа	содержание современных научных идей в рабочей области анализа	современных научных идей в рабочей области анализа, способен их сопоставить	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 преподавателям (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	**Семинар Лаборат. Практич.**	**Самост. работа**			
1	**Основы криптографии**	**8**	4	6	10	Ответ на экзамене. Отчеты по лабораторным работам	10/6	ОПК-3
2	**Криптография, виды шифрования**	**8**	4	4	12	Ответ на экзамене. Отчеты по лабораторным работам	8/4	ОПК-3 ПК-8
3	**Шифрование с ключом**	**8**	4	4	12	Ответ на экзамене. Отчеты по лабораторным	8/4	ОПК-3 ПК-8 ПСК-7.5

						работам		
4	**Алгоритмы, методы и средства обеспечения конфиденциальности, подлинности и целостности информации**	**8**	4	4	12	Ответ на экзамене Отчеты по лабораторным работам	8/4	ОПК-3 ПК-5 ПК-8
5	**Модели шифрования и дешифрования**	**8**	2	6	12	Ответ на экзамене. Отчеты по лабораторным работам	8/6	ОПК-3 ПК-5 ПК-8 ПСК-7.5
6	**Стойкость криптографической системы**	**8**	4	6	12	Ответ на экзамене. Отчеты по лабораторным работам	10/6	ОПК-3 ПК-5 ПК-8 ПСК-7.5
7	**Аддитивные шифры**	**8**	2	6	12	Ответ на экзамене. Отчеты по лабораторным работам	8/6	ОПК-3 ПК-5 ПК-8
8	**Ленточные шифры**	**8**	2	4	12	Ответ на экзамене. Отчеты по лабораторным работам	6/4	ОПК-3 ПК-5 ПК-8
9	**Блочные шифры симметричные и несимметричные**	**8**	4	4	12	Ответ на экзамене. Отчеты по лабораторным работам	8/4	ОПК-3 ПК-5 ПК-8
	ИТОГО		30	44	106		74/44	

4.2. Содержание разделов дисциплины

4.2.1. Основы защиты информации.

Информация как объект защиты. Информационная безопасность Российской Федерации. Направления защиты информации. Система защиты информации. Основные мероприятия по защите информации. Мероприятия по контролю эффективности защиты информации

4.2.2. Техническая разведка.

Классификация технической разведки. Возможности видов технических разведок. Обработка разведывательной информации. Оценка возможностей технической разведки по добыванию информации. Характеристика разведывательного сообщества США

.

4.2.3. Технические каналы утечки информации.

Обобщенная модель технического канала утечки информации. Опасные сигналы. Классификация технических каналов утечки информации. Побочные электромагнитные излучения и зоны пространственной защиты информации. Демаскирующие признаки объектов защиты.

4.2.4. Средства выявления технических каналов утечки информации.

Индикаторы электромагнитного поля. Сканирующие радиоприемники. Автоматизированные комплексы радиоконтроля. Комплексы оценки защищенности технических средств по каналу ПЭМИН. Комплексы оценки защищенности информации от утечки по акустическому и виброакустическому каналам. Многофункциональный комплект для выявления каналов утечки информации «Пиранья». Нелинейные локаторы. Металлодетекторы. Портативные рентгено-телевизионные установки. Досмотровые эндоскопы

4.2.5. Защита информации от утечки по техническим каналам.

Экранирование электромагнитных полей. Заземление технических средств. Фильтрация информационных сигналов. Маскирование информационных сигналов ПЭМИН. Маскирование акустических речевых сигналов

4.3. Семинарские, практические, лабораторные занятия, их содержание

№ п/п	№ раздела дисциплины	Тема занятия	Форма проведения	Формируемые компетенции
1	1	Исследование шифра простой замены	Лабораторная	ПК-14
2	2	Исследование шифра перестановки (шифр кардано)	Лабораторная	ПК-19, ПК-20
3	3,4	Исследование полиалфавитных шифров	Лабораторная	ПК-19, ПК-20
4	5,6	Исследование шифров многобуквенной замены	Лабораторная	ПК-24, ПК-35
5	7	Исследование шифра гаммирования	Лабораторная	ПК-19, ПК-25, ПК-20
6	8	Классическая сеть файстеля	Лабораторная	ПК-19, ПК-25, ПК-20
7	9	Исследование криптоалгоритма шифрования эль-гамаля	Лабораторная	ПК-19, ПК-25, ПК-20
8	9	Электронная цифровая подпись на основе задачи сложности дискретного логарифмирования	Лабораторная	ПК-19, ПК-25, ПК-20

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 проверки и защиты отчетов лабораторных работ.

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:

1. Методические указания по выполнению лабораторных работ.
2. Дополнительный лекционный материал

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

Источники для самостоятельной подготовки:

1. Технические средства и методы защиты информации от утечки по техническим каналам на объектах информатизации: учебное пособие. А.Е. Давыдов, Р.В. Максимов, О.К. Савицкий. – СПб.: Изд-во Политехн. ун-та, 2012. – 192 с.

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.Комбивирующий поточный шифр с элементом памяти
16.Моцификация сети Файстеля дня большего числа ветвей: тип 2 и тип 3. 1
17.Шифры многоанфавитиой замены. Табло Вижепера
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. Іифры перестановки. Квадрат «Кардана».
33. MARS структура: образующая функция, схемы входного и выходного перемешивания.
за. 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 _____ Бурлов В.Г.

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. Лось, А. Б. Криптографические методы защиты информации : учебник для академического бакалавриата / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — М. : Издательство Юрайт, 2018. — 473 с. — (Серия : Бакалавр. Академический курс). — ISBN 978-5-534-01530-0. — Режим доступа : www.biblio-online.ru/book/27397D56-C8A1-4970-9F39-28E7FA40632A

3.Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для академического бакалавриата / В. М. Фомичёв, Д. А. Мельников ; под ред. В. М. Фомичёва. — М. : Издательство Юрайт, 2018. — 209 с. — (Серия : Бакалавр. Академический курс). — ISBN 978-5-9916-7088-3. — Режим доступа : www.biblio-online.ru/book/C0328DC2-2A46-4945-994F-04F661095B83

4.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

5.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.

6. 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. 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.

2. 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.

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:

https://biblio-online.ru – ЭБС Юрайт;

http://elib.rshu.ru/ - ЭБС ГидроМетеоОнлайн структурная часть фонда библиотеки РГГМУ

http://www.prospektnauki.ru - ЭБС издательства «Проспект науки»

http://znanium.com – ЭБС znanium.com

www.intuit.ru – Национальный открытый университет

www.inf1.info/ - Планета Информатики

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

Те	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
Основы защиты информации	Лабораторные работы Технология объяснительно-иллюстративного обучения	MS Office 2007
Техническая разведка	Лабораторные работы	MS Office 2007 Internet Explorer
Технические каналы утечки информации.	Лабораторные работы	MS Office 2007
Средства выявления технических каналов утечки информации.	Лабораторные работы	MS Office 2007
Защита информации от утечки по техническим каналам.	Лабораторные работы	MS Office 2007

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

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

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

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).